

كيف اقتُحِمَت السرِّيَّةُ في العصر الرقمي

ستيفن ليفي

مؤلف كتاب قراصنة الكومبيوتر

تعريب : عبد الاله الملاح

مكتبة العبيكان



كيف اقتُحِمَت السرِّية في العصر الرقمي

ستيفن ليفي

تعريب

عبد الإله الملاّح

مكتبة العبيكان

الشيفرة

First published in the United States under the title:

CRYPTO

By Steven Levy

Published by arrangement with Viking Penguin, a division of Penguin Putnam Inc.

حقوق الطبعة العربية محفوظة للعبيكان بالتعاقد فايكنغ بنغوين في نيويورك

الرياض 11452، المملكة العربية السعودية، شمال طريق الملك فهد مع تقاطع العروبة، ص.ب. 6672
Obeikan Publishers, North King Fahd Road, P.O.Box 6672, Riyadh 11452, Saudi Arabia
الطبعة العربية الأولى 1423 هـ - 2002م
ISBN 9960-40-127-8

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

ليفي، ستيفن
الشيفرة: كيف انتُجِمَت السِّرِّيَّة في العصر الرقمي - تعريب: عبد الإله الملاح
552 ص، 17 × 24 سم
ردمك: ISBN 9960-40-127-8
1 - أمن الكمبيوتر - كريبتوغرافيا
أ - الملاح، عبد الإله (تعريب) ب - العنوان
ديوي 081 5084 - 22 رقم الإيداع: 5084 - 22

ردمك: ISBN 9960-40-127-8

الطبعة الأولى 1 2 3 4 5 6 7 8 9 10

إِلى تريزا وأندرو

تنويه

يستند كتاب «الشّيفرة» Crypto إِلىٰ سلسلة من المقابلات التي أجريتها على امتداد العقد الماضي، مع أهالي عالم الكتابة بالشّيفرة «الكريبتوجرافيا» Cryptography، أَو من كان لهم تأثير فيه. ومن الواضح أن أعمق ما أحمل من الشكر هو حق لأولئك الذين بذلوا الكثير من الوقت والاهتمام لإنسان غريب عن عالمهم، أراد أن يقدِّم لقرَّائه تقريراً صحفياً جيداً. وجلّ أملي ألا ينتاب من أعانوني شعور بالاستياء إن أشرت إِلىٰ قلّة منهم تجاوزوا حدود الواجب في بذلهم العون، والمساعدة ومنهم: لين أدليمان، جيم بيد زوس، ديڤيد تشوم، هويتفيلد ديفي، ماري فيشر، إيريك هيوز، تيم ماي، راي أوزي، رون رايفست، فيل زيمرمان.

ولقد كنت في الفترة ما بين أيلول/ سبتمبر 1994 وحزيران/ يونيو 1995، زميلاً في مركز دراسات منبر الحرية الإعلامي، وكان مقرّه يومذاك في حرم جامعة كولومبيا. وإني لأقر، بكل حمية واندفاع، بما نلته من حدب من «منبر الحرية»، وتوفير لأسباب الراحة والمساعدة من هيئة مركز الدراسات الإعلامية، وما حظيت به من صحبة رائعة وحكمة جاءت في الوقت المناسب من أصدقائي الزملاء. ولقد أسعفني الباحث كاوشيك أروناجيري، الذي عملت وإياه هناك

بعدد لا يحصى من الوثائق، كما كان عوناً لي في بعض مجالات الرياضيّات. كذلك تفضل جون كاسدان فأتاح لي حضور مقرره في قانون السبرنطيقا، فضلاً عن مات بليز وجوان فيجينباوم اللذين أحاطاني برعايتهما حين أتاحا لي حضور مقرّرهما في علم الحاسوب وتطبيقاته في الكريبتوجرافيا.

ولقد أتاح لي كل من مارك روتنبيرج، وديفيد بانيسار، وديفيد سوبل، من مركز سرِّيَّة المعلومات الإلكترونية، الإطلاع على وثائق مذهلة حصلوا عليها من الحكومة ببراعتهم في استخدام قانون حرية الاستعلام. كما أرسل لي روجر ثلافلاي رزمة ضخمة من الوثائق ذات الصلة بـ آر إس إيه RSA [الأحرف الأولى من أسماء العلماء رافيست وشامير وأدليمان. هـ. م] وسايلنك Cylink. وقد بعث إلي سيمبسون جار فينكل بالبريد الإلكتروني مدونات مقابلات كان قد أجراها ليرفد بها كتابه الموسوم پي - جي - پي P.G.P. [منتهى السرِّيَّة Pretty Good Privacy] أما الآخرون الذين وفَّروا لي المساعدة هنا، ولم يُشر إليهم، فلهم مني جزيل الشكر أيضاً.

وكنت قد كتبت في السنوات الثماني الأخيرة عدداً من المقالات المطوّلة في موضوع الشّيفرة، وبعضها مبثوث في هذا الكتاب، خاصة تلك المقالات التي نشرت في مجلة وايرد Wired. بدأت بالتحقيق الرئيس حول موضوع «زعران الشّيفرة» Cypher Punks في عددها الثاني، وانتهت بأول رواية تفصيليَّة حول التشفير غير السرّي عام 1999. ويجدر بي أن أخصّ بالشكر كافّة رؤساء التحرير الذين عملت معهم في تلك المجلّة، وبالأخص كيفن كيللي. وكنت قد أجريت عدة تحقيقات حول موضوعات تتّصل بالشّيفرة، في مجلة ذي نيويورك تايمز، صندي مجازين، وماك وورلد، ونيوز ويك. وكانت هذه الأخيرة مقرّي المهني طوال السنوات الخمس الأخيرة، وإني لممتن لكل من في هذا المقرّ لتوفيرهم حافزاً لكاتب أدمن العمل الحرّ، ليرتبط بوظيفة ويصبح أحد أفراد أسرة التحرير. وبعد، فإني أتوجّه بالشكر لمارك هويتكر وجون متشام وجورج

هاكيت المحرِّر الذي عانى مني الأمرّين. كذلك أجدني أقرّ بدَين عظيم للراحل مينارد باركر.

وفي دار النشر فايكينج، وجدت المحررة «بام دورمان» تستمر بقوة وحزم في سباق الماراتون لإنجاز الكتاب. كذلك كان «لآن ماه» الفضل في حثّي على متابعة العمل، كما وجدت «فيكتوريا رايت» مجلية في نقل المادة إلىٰ نصوص مطبوعة متحلّيةً بدقة الملاحظة. أما وكيل أعمالي فليب بروفي فقد وجدت فيه من جديد الناصح المدقِّق الأمين والميسِّر للعقبات. وقد أفادني بعض من تفضّلوا بقراءة المخطوطة، بالتنبيه للأخطاء وتقديم بعض المقترحات القيِّمة (ولن أشير إليهم بالاسم، فأنا وحدي المسؤول عن كل خطأ). وإني لأهيب بمن يقع على المزيد من المقترحات، أَو يعثر على أخطاء أخرى، أن الإتصال عبر موقعي على الإنترنيت www.Steven Levy.com حيث أدرج التصويبات والمستجدّات.

إن الكلمات لتقصر، حتى بأفصح العبارات، عن التعبير عما أدين به لأسرتي، أندروا وتيريزا.

ستيڤن ليڤي، أيلول/ سبتمبر 2000

المحتوى

الشيفرة

تصدير

لقد جعل البرق، والهاتف، والمذياع، وبالأخص الكومبيوتر، كل من على الكرة الأرضية على مسمع من بعضهم البعض، وكان الثمن من خصوصيتنا. ولعلّنا نشعر بأنّنا نقوم بعمل حميمي حين نلتقط الهاتف الخلوي، أَو ننكبّ على الحاسوب، دونما تكلّف، ونحن معزولون في غرفنا وبين جدران مكاتبنا الضيّقة، لننقل أفكارنا ، وأسرارنا، ومشاريعنا العمليَّة، بل حتى أموالنا. إلاَّ أن متنصتاً ذكياً بل غير ذكي أيضاً، قادر على الإحاطة بما يدور بين الناس. وقد نحسب أننا بالهمس نفوّت على الآخرين إمكانية سماع ما يدور بين بعضنا البعض، إِلاَّ أننا، في الواقع، إنما نذيع أخبارنا على الملأ.

ومع ذلك فثمة ترياق يعد بالخير: أعني الكريبتوجرافيا، أي استخدام الرموز السرِّيَّة والشّيفرة لتعمية المعلومات، بحيث لا تفيد سوى المتلقي المعني بالرسالة. وعبر سحر الكريبتوجرافيا أخذت الاتِّصالات التي تتمّ في عالم الواقع، من تواقيع وعقود وإيصالات إِلىٰ ألعاب البوكر، تبلغ طريقها إِلىٰ كافة مستخدمي الأَجهزة الإِلكترونية الشائعة اليوم. ولكن سرعان ما ساد، منذ أوائل السبعينات، سكون يصمّ الآذان أحاط بهذه التكنولوجيا المذهلة. فقد استطاعت الحكومات، وخاصة حكومة الولايات المتّحدة، إخماد النقاش المفتوح حول أي جانب من هذا الموضوع يتعدّى العلم الذي يتلقاه الفتيان في مدارسهم.

وبات مآل من ينشد تناول الموضوعات الأساسيَّة في الكريبتوجرافيا، أَو يحاول ابتكار رموز جديدة أَو تفكيك القديمة، وهذا هو الأسوأ، إِلىٰ البحث وحيداً في عزلة عن الناس مما يؤدي عادة إِلىٰ الأبواب الموصدة، أَو قطع الاتِّصالات الهاتفية فجأة، أَو حتى التحذيرات والنصح بالالتفات إِلىٰ التفكير بأمور أخرى.

إن لخطر الدخول في موضوع الشّيفرة منطقاً سليماً يقول: لما كانت السرِّيَّة هي الجوهر والمبتغى من الكريبتوجرافيا فمن شأن أقل خيط من ضوء الشمس، بما يترتب عليه من كشف للأسرار، أن يكشف شيفرة الحكومة، مما يلحق بها ضرراً مأساوياً. فالغريب الذي يلم بأسلوبنا في التشفير encryption قادر بلا ريب، على ابتكار رموزه الخاصَّة؛ كذلك العدو العارف بالرموز التي نستطيع تفكيكها، يستطيع أن يستبعد تلك الرموز، حالما يتوصَّل إِلىٰ هذه المعرفة.

ولكن ماذا لو أن هناك جهات أخرى، غير الحكومات، تفيد من الكريبتوجرافيا؟ ثم ماذا لو أن النَّاس أنفسهم على وجه العموم كانوا يحتاجون إلى هذا العلم، لحماية مراسلاتهم واتِّصالاتهم وبياناتهم الشخصيَّة Personal data، من تطفّل المتطفلين كافة، ومنهم الحكومة ذاتها؟ أفليست الحرية الخاصَّة حق لكل إنسان؟ ثم أفلا يعني ظهور الاتِّصالات عبر الكومبيوتر أن لكل إنسان حرية استخدام الأجهزة الراقية المعقَّدة التي تتيح لهم تبادل الكلام مع المحامين والأحبة، والزملاء والزبائن، والأطباء ورجال الدِّين بذات القدر من الأمان الذي توفِّره المقابلة الشخصية والأحاديث خلف الأبواب المغلقة؟

إن هذا الكتاب يروي قصة الناس الذين طرحوا هذه التساؤلات وأوجدوا ثورة في الحقل المقدّر له أن يُحدث التغيير في حياتنا جميعاً. وهذه، بعد، قصة أولئك الذين بذلوا أقصى ما لديهم لتبديد هذه التساؤلات. أما من تقدّم ذكرهم فهم أشخاص عاديّون لا شأن عظيماً لهم: المشتغلون بالحاسوب، والأكاديميون، وأهل السياسة، والقادة العسكريون ورؤساء الدول. فمن يا تُرى، إذن، قد كسب في هذه المعمعة؟

المتفرّد

نفرت ماري فيشر من هويتفيلد ديفي حين وقع نظرها عليه؛ فقد كان من نمط تعرفه أحسن المعرفة؛ رجل من نوابغ معهد ماساتشوسيتس التكنولوجي (إم آي تي MIT)، عليه مسحة من العجرفة، هي ستار من الدخان، يخفي وراءه قدراً عظيماً من اضطراب الشخصيَّة. وكان لقاؤهما سنة 1969، والمكان مخزن بالقرب من الساحة المركزية في كيمبريدج بولاية ماساتشوسيتس. وكان يحمل على كتفه يومذاك شريطاً طويلاً يبدو وكأنَّه يريد أن يربط به أحد الحيوانات الأليفة. وكان ذلك من الأشياء التي اعتاد ديفي شراءها، وعرف باقتنائه مجموعة غريبة من الحيوانات، ومنها ثعبان الصخور الذي يبلغ طوله تسعة أقدام، وظربان، وحيوان نادر شبيه بالنمس يغطي جسمه فراء، ويفرز مادة تسبِّب الحساسيَّة، ويتغذَّى بالفئران الحيّة، ويشتهر بهجومه على البشر حيث يغرز في أجسامهم أنيابه الحادّة كالإبر، على حين غرّة، فيما هم يتأملونه معجبين. ولقد كان صاحب حيوان كهذا يحظى عادة باهتمام ماري فيشر المحبة للحيوانات، والتي كانت في تلك اللحظة تحمل في جيبها سنجاباً. كذلك كان لديها في بيتها ظربانٌ وكلبان وثعلب وطائر سحنون مغرّد ذو جناحين أبيضين، واثنان من دببة العسل التي تقطن جنوب أمريكا. ولقد استرعت المرأة انتباه ديفي حين رآها تشتري بعض المشابك لأقفاص الحيوانات، فأخذ بملاحظتها دون سواها.

قدر لديفي أن يُعرف ـ وتذيع شهرته ـ في السنوات اللاحقة باعتباره مشاركاً في اكتشاف المفتاح العام للشيفرة، وظهر بشعره الأشقر الطويل المنسدل على كتفيه، ولحيته التي تذكر [ببطل الغرب الأمريكي] بفلو بيل، وملابسه المصنوعة حسب الطلب بيد خياطي لندن، بصورة مهيبة وكأنَّه أحد الشخصيَّات التي تصورها الأيقونات. أما في تلك الأيام، فكان ما يزال فتى حليقاً على حد تعبير ماري فيشر، وأخذ يومئذ يمطرها بوابل من الأسئلة. هل تربين حيوانات غريبة؟ إذن فسوف تحتاجين إِلىٰ هذا، ثم هذا، ثم هذه. وكان يأخذ ما تحمله بيديها، ويضع بدلاً منه أشياء أخرى، فيما هو مستمر في محاضرته. ولقد شعرت ماري بالضيق لما بدا منه من فجاجة، ولكنها لم تكن قد تمكنت، بعد، من فكّ رموزه.

لم تكن ماري فيشر تعلم أن ديفي يمضي أوقاتاً طويلة في التفكير في قضايا تتّصل بأمن الكومبيوتر ومضامينه الرياضيَّة. ولم يكن لديها أي فكرة عن انشغاله بالبحث عن طرق جديدة للحفاظ على الأسرار. وجلّ ما علمت من أمره أنّه رجل منفّر يهوى الحيوانات. أما الحيوانات، فكانت مصدر شغف لماري، وما هو إِلاّ حين، حتى أخذ ديفي وصديقته بزيارتها وزوجها وبصحبتهما حيواناتهما أحياناً. وكان أن توافقت الظرابين، وتم تبادل بعض الحيوانات من فصيلة القرقدون، وأصبحت زيارات ديفي لمنزلها أمراً معتاداً.

أخذت ماري تعيد النظر في شعورها بالنفور من ديفي الذي تملّكها حين التقت به أوّل مرة. أما هو، إذ عجز عن فهمها، فقد بدا ساهياً عنها. فكان يقتصر في محادثاته أثناء تلك الزيارات على رجل البيت. ولما انتقلت ماري وزوجها إِلىٰ نيوجيرسي، حيث أنشأ الرجل هناك كلية لطب الحيوان، أصبحت ماري ترد على الهاتف بين الحين والآخر لتجد أن المتكلم ديفي بصوته الدقيق المتأنّي والحازم، يطلب زوجها دون أن يسأل عنها، وكأنها آلة وظيفتها الرد على المتكلّم. وفي ذات يوم، كان السيل قد بلغ الزبى بالمرأة، فلم تتمالك

نفسها عن الإفصاح بمشاعرها، وردت عليه بقولها: «اسمع: أعرف أن ذكائي لا يعادل ذكاءك وذكاء بعض أصحابك، وأدرك أن صداقتك أساساً مع زوجي. لكني لا أعتقد أن كلمة «مرحباً» يمكن أن توردك موارد التهلكة».

ولقد فعلت تلك الكلمات فعلها، فتحسّن سلوك ديڤي حيال ماري تحسّناً عظيماً، حتى أنها لم تُدهش حين أخبرها ذات يوم من عام 1971 أنَّه سيغيب في رحلة بعض الوقت، بل شعرت بالحزن أيضاً. ولم تكن ماري تعلم، بعد، أن ديڤي يستعد للقيام ببحث بطولي منفرد، يتقصَّى إجابات عن أسئلة لا ترغب حكومة الولايات المتّحدة لأحد أن يطرحها. وكانت احتمالات الفشل في هذا المسعى أضخم من أن تحصى، ذلك أن الرجل كان يواجه ما يكاد يكون خطراً تاماً يحول دون اطلاعه على المعلومات المتصلة بموضوع هو، في مستوياته الدقيقة المعقّدة، غامض أصلاً أشد الغموض. وبعد، فما نصيب مثل هذا الغريب المجهول في أن يأتي باكتشاف أصيل، لم يأت بمثله أحد من قبل، ليحدث انقلاباً في مفاهيم السرِّيَّة الشخصية في زمن الحاسوب.

لكن القائمة الطويلة لهذه العقبات قدّر لها أن تصبح أقصر بفضل الدور الذي كان لعلاقة ديڤي بماري فيشر، وما أدّت إليه من إنطلاقة علمية تمس كل مواطن في العصر الرقمي Digital age. وقد وصفت ماري فيشر ذلك قائلة: «كان اكتشاف المفتاح العام مغامرة عاطفية».

ولد بايلي هويتفيلد ديڤي عشية إنزال قوات الحلفاء على ساحل النورماندي، في 5 حزيران/ يونيو 1944. وكان والده قد أكمل لتوه سنة من الخدمة في الحكومة أثناء فترة الحرب (وإن يكن ديڤي يبغض الشيوعيين، لتعصبهم وجفاف طبعهم أكثر مما يبغض عقيدتهم، فإن والده كان مناهضاً للفاشية، وكثيراً ما كان يحاضر في مناهضة حركة القمع في أوروبا). وكان والدا ديڤي على درجة عالية من الثقافة. فقد درس والده بايلي والاس ديڤي، تاريخ شبه الجزيرة الأيبرية وحضارتها في كلية سيتي كوليج في نيويورك. أما

والدته، جوستين لويس هويتفيلد، فكانت ابنة لأحد تجار البورصة في ولاية تنيسي، والتقت زوجها أثناء عملها في السلك الديبلوماسي في إسبانيا، وكانت كاتبة وعالمة، فقد درست حياة مدام دو سيفينييه الشخصية البارزة في بلاط لويس الثالث عشر والرابع عشر.

كان هويت ديفي دائماً شخصية مستقلّة. وكما لاحظ أحد أصدقائه في بواكير حياته: «كان للطفل أسلوبه الخاص في الحياة، وهو بعد في الخامسة من عمره». ولم يتعلّم ديفي القراءة حتى بلغ العاشرة. ولم يكن السبب في ذلك صعوبة يعاني منها، فالمسألة أنّه كان يؤثر أن يقرأ له أبواه، ويبدو أنَّهما كانا يصبران على ذلك. وأنهما كانا يعيان مبلغ ذكاء ولدهما وشدّة تفرّده، فلم يشاءا حمله على ما يكره. وفي النهاية، وفي الصف الخامس الابتدائي، وقع على كتاب بعنوان «قطة الفضاء»، وشرع بدراسته دونما مرشد، ثم انتقل فوراً إِلىٰ قراءة حكايات «ساحر اوز».

ويذكر ديفي، بعد عقود من الزمن، أن معلمته في ذلك العام: «كان اسمها ماري كولينز، وأود أن ألقاها، إن كانت ما تزال حيّة»، فقد أمضت، مرةً، ما بعد الظهر في أحد الأيام، لتشرح أمراً قُدِّر له أن يلازمه ردحاً طويلاً، هو أُسس الكريبتوجرافيا. وحرصت على أن تبين له كيف يمكن للمرء حل ما يُعرف بالشّيفرة البديلة.

ولقد وجد ديفي في لكريبتوجرافيا وسيلة تآمرية ممتعة للتعبير، حيث يتواطأ مستخدمو هذه اللغة فيما بينهم للحفاظ على أسرارهم في عالم حافل بعيون المتطفلين. ويتجلّى ذلك بأن يعمد المرسل إِلىٰ تحويل رسالة خاصة إِلىٰ وضع آخر، بحيث تصبح ضرباً من اللغة الغامضة وهذا ما نسميه: التشفير encryption. فإذا تحوَّلت الرسالة إِلىٰ ما يشبه الهذيان، انتهى من يود التنصّت إِلىٰ الفشل وأحبط مسعاه. وليس هناك من يستطيع أن يعيد الرسالة إِلىٰ حالها الأول من الانسجام إِلاَّ أولئك الذين يملكون قواعد تحويل الرموز إِلىٰ كلام

مفهوم كما كان سابقاً: أي فك التشفير decryption. أما الذين لا يملكون هذه المعرفة ويحاولون فك شيفرة الرسائل دون «المفاتيح» السرِّيَّة، فإنَّهم يعتمدون على تحليل الشّيفرة Cryptanalysis.

إن الشّيفرة البديلة هي ابتكار أحدهم للنص المشفر Cipher text (الرسالة المعماة)، عن طريق استبدال حروف الرسالة الأصلية، أَو النص الواضح Plain text، بحروف أخرى وفق خطة متفق عليها مسبقاً. وأبسط شكل لها ما يُعرف بشيفرة قيصر، ويُعتقد أن يوليوس قيصر استخدمها وإليه تُنسب. ويعتمد هذا النظام في كتابة الشّيفرة، على نقل كل حرف في النص الأصلي إِلىٰ الأمام بالحرف الثالث الذي يليه من حروف الهجاء (مثال ذلك يستبدل الحرف A بـ D وB بـ E وهكذا. . .) وهناك أيضاً أسلوب أشد تعقيداً يكلّف محلّل الشّيفرة بعض الجهد، ويقوم على استبدال الحرف بنظير له في قائمة حروف هجاء أخرى موجودة لدى المتلقي، ومنسقة بطريقة عشوائية خاصة. وجدير بالذكر أن الصحف، كثيراً ما تنشر نصاً مشفراً Cryptogram يومياً لقول مأثور أَو مقتطفات تلخص قولاً مطولاً على هذا النحو. وهذا أسلوب يسهل حله إِلىٰ حد بعيد بسبب تكرار حروف معينة على نحو منتظم وتوزيع الكلمات بطريقة، غالباً ما يسهل التنبؤ بها.

افتتن هويت ديفي، شأنه شأن عدد لا يحصى من الفتيان من قبله، بهذه العملية. ولعلّنا نرجع إِلىٰ ديفيد كاهن في تأريخه للكريبتوجرافيا، في كتابه مفكّكو الشّيفرة The Code breakers الذي يستقصي فيه الدوافع العاطفية وراء الكتابة السرِّيَّة، ويعتمد فيه على نظريَّة فرويد في ارتباط الدافع للتعلّم عند الطفل بالرغبة بالتعرّف إِلىٰ الممنوع. ونجده يقول: «إنّك ستحاول، إن كنت ذكراً، أن تتعرّف إِلىٰ ما تخفيه الأنثى تحت ثيابها. وإذا شئت الحقيقة البسيطة، فإن ذلك مردّه الرغبة في المعرفة». كذلك يجد الكثيرون أن سحر الشّيفرة، يتّصل بالمتعة المتأتية عن تفكيك الرسائل المشفَّرة. وكل نص مشفّر يقع عليه المرء هو،

بالنتيجة، دعوة له ليقوم بدور المتنصّت، أَو المتطفل، أَو المتلصص.

وعلى أي حال، فإن فكّ الشّيفرة، لم يكن مصدر الإثارة لهويت ديفي، وإنما الاهتمام الأكثر مواربة في إيجاد شيفرة لحماية المعلومات؛ وهو يقول الآن: الحق أني لم أكن حاذقاً في حل الألغاز، ولا عملت كثيراً في حل الشيفرة سواء في تلك الأيام أَو فيما بعد. ذلك أنّه كان يؤثر دائماً الحفاظ على الأسرار على اختراق أسرار الآخرين.

كانت استجابة ديفي للدرس الذي تلقّاه من الآنسة كولينز في الكريبتوجرافيا، الاستجابة المألوفة منه. فقد أهمل القيام بما كلّفته به من واجبات دراسيَّة، والتفت ليتابع الموضوع ويتوسع في دراسته، دونما عون من أحد، وبطريقته المنهجيَّة وبدأب لا ينقطع. وكان ما أثار اهتمامه خصوصاً ملاحظة عابرة قالتها، وهي أن ثمة شيفرات أشد تعقيداً مثل «نظام الشّيفرة الأمريكية» التي لا يمكن اختراقها. وقد رجا هويت والده أن يبحث له في مكتبة الكلية عن الكتب التي تتعلّق بالكريبتوجرافيا. وسرعان ما عاد بايلي ديفي حاملاً رزمة ضخمة من هذه الكتب، ومن بينها كتابان مخصّصان للأطفال، فالتهمهما الفتى بسرعة، لكنّه وجد صعوبة كبيرة في كتاب هيلين فورشيه جاينز «تحليل الشّيفرة»، وهو كتاب على قدر لا بأس به من العمق ويعود تاريخ إصداره إلى عام 1939. فأقبل على دراسته بتأنٍ واهتمام.

وفي هذا الكتاب طرحت جاينز، مجموعة من التحديات الجيدة التنظيم، والتي توفر للهواة الجادين معرفة بأنظمة الكريبتوجرافيا الكلاسيكيَّة، والعديد منها تعديلات للتطوير الذي أجري عليها على مدى قرون، وهذه بدورها أكثر تعقيداً من الشيفرات التي سبقتها. وكان أشهرها النظام ذو الأبجدية المتعدّدة Polyalphabetic. والذي وُضع لأول مرّة في الأقبية السرِّيَّة تحت أرض الفاتيكان، ثم أعلنه في أوائل القرن السادس عشر قس ألماني يدعى يوهانس ثريثيميوس. وقد عرض هذا القس في كتابه المسمّى «بوليجرافيا» Polygraphia

الذي نُشر عام 1518 ـ بعد سنتين من وفاة مؤلّفه ـ طريقة استخدام الجداول التي يختص فيها كل حرف هجائي، بسطر بعد تغيير موقعه في التسلسل الألفبائي. فإذا أردت أن ترمِّز encode رسالتك، كان عليك وفق هذا النظام أن تحوِّل الحرف الأول منها، إلىٰ ما يقابله في السطر الأول من الجدول. وتتكرَّر العملية مع الحرف الثاني، بما يقابله في السطر الثاني، وهكذا دواليك.

ثم جاء دبلوماسي فرنسي يدعى بليس دوڤينير، في القرن السادس عشر، وسار في هذا السبيل على خطا ثريثيميوس. وفيه نجد رجلاً اخترق روح الكتابة السرِّيَّة. وقد وجدناه يقول ذات مرة: «كل ما في العالم مختزن في شيفرة، وما الطبيعة إلاَّ مجرد شيفرة وكتابة سرِّيَّة». ثم عرض في أشهر كتبه، التي تبلغ حوالي الأربعة وعشرين كتاباً، وضعها بعد تقاعده من الخدمة الدبلوماسيَّة، تطويرات مذهلة لأنظمة البوليجرافيا، وزاد فيها تعقيداً مضيفاً إليها جداول يصعب التنبؤ بها، و«مفاتيح ذاتية» تجعل من نص الرسالة ذاتها مفتاحاً لقراءة مضمونها. ولقد خلد ذكر النظام الذي وضعه دوفينير بسبب تماسكه وصعوبته على الحلّ، فعُرف بـ «الشّيفرة المنيعة»، وظلّ بعض الضليعين بالكريبتوجرافيا يعتقدون، حتى القرن العشرين تقريباً، أن من المستحيل إيجاد نظام يتجاوز ما أبدعه دو فينير.

والواقع أن فنون الكتابة السرِّيَّة حين تعرّف إليها ديڤي، كانت قد تطوّرت واختلف حالها كل الاختلاف عما كانت عليه في عصر دوفينير. ومع ذلك، فإن تساؤلات ديڤي الطفوليَّة جعلته يعتقد، بأن دوفينير خاتمة القول في هذا الموضوع. وإذ تملكته الفكرة بأن الكريبتوجرافيا مشكلة محلولة، فقد توقف عن متابعة قراءة كتاب جاينز. ثم أخذ الهوس الذي تملكه في موضوع الشّيفرة يتلاشى. وزاد من إعراضه عن متابعة هذا الموضوع ما رآه من اهتمام «الناس كلهم» بالرموز والشّيفرة، مما بدا له، وهو المشاكس الأصيل، «ضرباً من الابتذال» كما قال في وقت لاحق. فانتقل لدراسة «التحصينات في العهود

القديمة والخرائط العسكرية وفنون التمويه، والغازات السّامّة والحرب الجرثومية». ثم وجد جماعة صغيرة من أصدقائه الفتيان يشاركونه اهتماماته، بل إنه أخذ يتطلع للانتساب إِلىٰ القوّات المسلّحة، وراح يبحث عن الجامعات التي تشمل مناهجها دورات لتدريب ضبّاط الاحتياط. لكن واحداً فقط من تلك المجموعة ذات الاهتمامات العسكرية، انتسب إِلىٰ القوّات المسلّحة فعلاً، ومات في فييتنام.

كانت الرياضيات، لا الأسلحة الناريّة، هي التي حسمت الأمر في اختيار ديفي للجامعة. وقد وجد في الرياضيّات يومئذ أمراً لم يجده في التاريخ: الحقيقة المطلقة. وتفسر ماري فيشر ذلك بقولها: «أعتقد أن البحث عما هو حقيقة فعلاً، كان أحد المشاغل الأساسيّة في حياة هويت». وتروي أن والده استدعي إِلىٰ المدرسة والفتى ما زال في بواكير حياته لإعلامه أن ولده عبقري. وكان رد فعل بايلي ديفي، حسب رواية فيشر، أن خرج بحيلة أملاً منه بأن يؤدي ذلك إِلىٰ فرض نظام على الفتى يحكم مسلكه. فقال لابنه أنه دون الفتية الآخرين ذكاء، ولكنه قد يحقّق نتائج أفضل إن بذل جهداً أكبر مما يبذله أقرانه الأكثر ذكاء، والتزم بالجد والمثابرة. وتقول فيشر: «إن هذه الحيلة ربما كانت تجدي مع بعض الأطفال، أما في حالة هويت فكانت أسلوباً سيئاً، إذ أحدثت له صدمة ظلّ يعاني منها سنين عديدة، وفي ظني، أنها أحدثت في نفس هويت إحساساً بالتوق للحقيقة المطلقة».

ومع أن «هويت» كان تلميذاً نجيباً في المدرسة، إلاّ أنه لم يكن ليلتزم بالدراسة بالقدر الذي كان يرجوه والده. وكان مشاغباً أحياناً، ويجلي في المواد التي لا يشوبها الفرض والواجب. ويذكر عنه أن أستاذ مادة التفاضل والتكامل قال له ذات مرة، وقد سئم الشغب الذي كان يثيره في الصف: «لسوف تقوم ذات يوم بتحضير حلوى الخبيزة هنا!»، ولم يخيب هويت ظنّ المعلم، فحضر في اليوم التالي ومعه علبة من الصفيح ليطهو بها حلوى الخبيزة التي كان قد

أدخلها أحد أصدقائه خلسة إِلىٰ المدرسة. أما بما يتصل بالدراسة فإن ديڤي فشل في تحقيق المتطلبات اللازمة لنيل شهادة جامعية تامة، واقتصر على شهادة متواضعة تعرف بالدبلوم العام. بل لم يُقدر له أن يحضر حفل التخرّج إذ كان مسافراً بصحبة والده في رحلة إِلىٰ أوروبا. (كانت مأساة ديڤي الكبرى وفاة والدته أثناء دراسته الثانوية، وما زال إِلىٰ اليوم يتجنّب الحديث عن ذلك). ولم يتمكّن من دخول معهد ماساتشوسيتيس للتكنولوجيا عام 1961، إِلاَّ بفضل علاماته العالية في المواد التي تعتمد على كفاءة الطالب ومواهبه، كما بينت ذلك الاختبارات المعيارية التي طبقت من أجل قبول الطلاَّب في تلك الجامعة.

ويقول ديڤي معترفاً: «لم أكن بالطالب المتفوق حتى هناك في المعهد». غير أنه سحر بالقدرات العقلية التي يتمتع بها طلاّب المعهد، وهم مجموعة من المنبوذين اللامعين والملهمين والموهوبين الأفذاذ، وكان بعضهم يستطيع في دقيقة واحدة حل معضلة تستغرق من ديڤي نفسه يوماً بكامله. ولعل هويتفيلد ديڤي كان يبدو بين هؤلاء اللامعين أقلهم حظاً بأن يأتي بأمر خارق يغير من وجه التاريخ. ولكن لما كان أصحابه ذوو العقول الفذّة بشراً لا آلات جبارة، فقد اتخذت مصائرهم مسارات غير متوقعة. فانتهى بعض النخبة من هؤلاء الأفذاذ بالدوران في فلك ألعاب الكومبيوتر المعقدة أَو الترويج للعقاقير من الأعشاب، أَو تعليم التأمل.

ويستعيد أقران ديڤي في إم آي تي MIT صورته الحية في ذاكرتهم، فيتذكّرون الفتى الغريب الأطوار ذو الشعر الأشقر المنتصب فوق رأسه بطول بوصتين (يقول أحد أصدقائه يومذاك: «إذا شئت أن تشذب هذا الشعر فعليك بمقص الأعشاب»). وكان من عاداته أن يسير قفزاً في حرم الجامعة على رؤوس أصابع قدميه، وتلك الطريقة في السير عُرف بها دون الآخرين، وغدت علامة مميزة له كأنما هي توقيع متحرّك. إِلاَّ أنه عُرف أيضاً بعمق فهمه للرياضيَّات.

اختار ديڤي من مناهج الدراسة برمجة الكومبيوتر ليتفادى ـ على ما

يقول اليوم ـ الخدمة العسكرية. ثم يزيد: «كنت أحسب أن دراسة الكومبيوتر غير ذات شأن، وكنت أعتبر نفسي رياضياً صرفاً، وانصبّ اهتمامي على معادلات التفاضل الجزئي والهندسة اللاكمية (الطوبولوجيا) وما شابه. ولكنه حين نال شهادة التخرّج سنة 1965 من معهد ماساتشوسيتس، والحرب في فيتنام تدور رحاها، وجد نفسه زاهداً كل الزهد عن إغراءات الصراع المسلَّح، فتحوّل، حسب قوله، إلى «داعية سلام»، ناهيك عن غرابة الأطوار. وقد اعتاد العيش يومذاك مع صديقته في شقة صغيرة في كمبردج (بولاية بوسطن الأمريكية. هـ. م)، أخذت تزدحم بخزانات الماء الزجاجية لدى النباتات الغريبة التي كان يقتنيها. كذلك عرف ديفي بشغفه بالطعام الصيني، كما اشتهر بحمله عودين أنيقين من الخشب أينما ذهب، كما يفعل لاعب البلياردو الجاد بعصاه الأثيرة.

ومن أجل تفادي الخدمة الإلزامية. قبل ديفي العمل في شركة ميتري كوربوريشن، التي تختص بتعهدات وزارة الدفاع، وهي توفِّر لموظفيها الشباب وسيلة للتهرّب من الخدمة العسكرية. ولم يكن لعمله علاقة مباشرة بالمجهود الحربي، بل كان يعمل تحت إمرة عالم في الرياضيات يدعى رونالد سيلفر، ويشارك زميلاً آخر في وضع رزمة برمجيات Software Package تدعى «مختبر الرياضيات» Math lab، وقد طور هذا فيما بعد في نظام معالجة رياضي رمزي مشهور يُعرف بـ ماكسيما Macsyma(*). (ومع أن قلّة كانوا يعلمون آنذاك بطبيعة مساهمة ديفي، إلاّ أن الخبراء أدركوا أن عمله هنا يتطلَّب تفوّقاً في الحساب، ونظرية الأعداد، وبرمجة الحاسوب).

والأهم من ذلك كله، أن أعضاء فريق ديفي لم يكونوا ملزمين بالعمل في مكاتب الشركة، لكنه أصبح في عام 1966، ضيفاً مقيماً لدى مارفين

(*) Macsyma ماكسيما: لغة برمجية مصممة لمعالجة التغيرات الحسابية غير العددية هـ. م.

مينسكي، ذي المكانة السامية في مختبر الذكاء الاصطناعي في معهد ماساتشوسيتس للتكنولوجيا. ولقد ظل يعمل هناك طوال ثلاث سنوات، بات خلالها جزءاً من هذه التجربة التاريخية الممتعة لجعل الآلات ذكية، وتوسيع حدود برمجة الكومبيوتر، وترسيخ روح تبادل المعلومات كأساس لحضارة الكومبيوتر. وظهر أن جانباً من توجهات هذه الجماعة من متسللي الكمبيوتر الفضوليين، ذو صلة بالاتجاهات التي تنحو إليها اهتمامات ديفي. وكما أن ثمة كلمات شائعة في بعض اللغات دون أن يكون لها معنى في حضارة أخرى (ما حاجة مجتمع استوائي لكلمة ثلج؟) كذلك لم يكن لدى مختبر الذكاء الاصطناعي معادل تكنولوجي لكلمة «ملكية». فكان المفترض عندهم أن المعلومات ينبغي أن تكون متاحة كالهواء ذاته. وبالتالي لم يكن ثمة ما يقيد الاطلاع على برمجيات نظام التشغيل الذي وضعه المميزون في معهد ماساتشوسيتس للتكنولوجيا.

لكن ديفي، على أية حال، كان على العكس من أقرانه يؤمن بأن على التكنولوجيا أن توفّر للمرء شعوراً بالخصوصيَّة والسرِّيَّة. وبخلاف بعض زملائه المتسللين الذين كانوا يجدون أعظم المتعة في اللعب في مرابع الحاسوب المحرمة، وجد ديفي نفسه مهتماً بالبحث عن البرمجيات التي يمكن وضعها بحيث تحول دون اختراق المتطفلين ملفات الآخرين. وللحقيقة كان ديفي قد شارك في أعمال تفكيك رموز الرسائل السرِّيَّة، تلك الهواية الشائعة في مختبر الذكاء الاصطناعي: ومن الألعاب الشائعة أيضاً، اكتشاف الطرق لفتح الخزائن التي تُعتبر بالمعايير الحكومية، مأمونة. لكن ديفي كان يجد في حماية الخزانة المأمونة المتينة، متعة تفوق ما في كسر الأقفال من نظام ضعيف التصميم. وكان يحلو له إخفاء ما لديه في خزائن سرِّيَّة محكمة الإغلاق.

وفي عصر المعلوماتية، فإن القلعة الحصينة المأمونة للمعلومات، تكمن في البرمجيات Software لا في العتاد hardware: فهي خزائن حقيقية لحماية

البيانات الثمينة. ذلك أن المعلومات تمثّل، قبل كل شيء، كنز العصر الحديث، وهي تعادل قيمة القطع النقدية والحلي الذهبية في الحقب الماضية. وكان الحقل المناطة به هذه المسؤولية في تلك الأيام هو أمن الكومبيوتر، الذي كان ما يزال يومئذ في مرحلة الولادة. ولم يكن هناك كثيرون يكلفون أنفسهم عناء مناقشة مضامينه الفلسفية. أما ديڤي، فغالباً ما كان يخوض مع رئيسه في حوارات حول هذا الموضوع إلىٰ موضوع الكريبتوجرافيا.

كان لدى سيلفر بعض المعرفة في هذا الحقل، وقد كشف الرجل المجرب لديڤي، عن أمور ما كانت لتخطر له ببال، حينما درسها لوحده وهو في الصف الخامس. ففي أحد الأيام جلس الاثنان في المقهى في تيك سكوير Tech Square، ذلك البناء الشبيه بالعلبة ذو الطوابق التسعة، والذي يضم في العلوية منها، مختبر الذكاء الاصطناعي، وشرع سيلفر يشرح لديڤي بعناية ودقّة، أساليب عمل أنظمة الكتابة السرّيّة الحديثة.

وغني عن القول، أن هذه المنظومات تعتمد على الآلات، فهي التي تقوم بالعمل ـ سواء كانت أدوات كهروميكانيكية، مثل آلات شيفرة إنجيما Engima، التي استخدمها الألمان أثناء الحرب العالمية الثانية، أو منظومة موجهة بالكومبيوتر كما في عصرنا، حيث تقوم هذه الآلات بتمويه الرسائل والوثائق بواسطة وصفة فريدة تسمح بتغيير الرسالة حرفاً بحرف. (تقوم الوصفة على مجموعة من المعادلات الرياضية المعقّدة، الخوارزميات Algorithms). ولا يستطيع حلّ هذه الرسالة إلاّ من لديه آلة مماثلة أو برنامج كومبيوتر يتمكن من عكس العملية، وتحويل النص المشفر إلىٰ نص واضح، باستخدام المفتاح العددي الخاص الذي استخدم في تشفير النص أصلاً.

في حالة آلات الإنجيما، كان المفتاح يقوم على تعيين «مواقع» مختلف دواليب الرموز التي تحدّد كيفية تغيير كل حرف. فكان على كتّاب الشّيفرة إعادة ترتيب الدواليب كل يوم بشكل يختلف عن سابقه؛ ويعلم مستقبلو الرسائل سلفاً

بالمواقع المعينة للدواليب في ذلك اليوم. ولذلك كان العمل المنظم الدؤوب الذي جرى في بليتشلي بارك، في إنكلترا، وأدّى إِلىٰ فوز الحلفاء بآلات الإنجيما في عملية هي أهم إنجاز للحلفاء في مجال الاستخبارات، مجرد جانب من العملية المعقَّدة في حل رموز الرسائل السرِّيَّة. وكان على محلِّلي الشّيفرة أن يحيطوا بالصيغة التي يعتمدها خصومهم من قوّات المحور في ترتيب مواقع الدواليب؛ وإذا تم ذلك لهم، كان عليهم أن يقوّموا بما عرف بالهجوم بـ«القوة الغاشمة»، الذي يقتضي اختبار كل الاحتمالات الممكنة لترتيب المواقع ولا يمكن تنفيذ ذلك إِلاَّ بابتكار آلات هي أسلاف الكومبيوترات الحديثة.

أما بالنسبة للكومبيوتر، فإن المعادل لمواقع الإنجيما فمفتاح رقمي digital key، وهو شريط من الأرقام التي تساعد في تعيين النِّظام الذي يقوم بتحويل الرسالة الأصلية. ولا بدّ لمتلقّي الرسالة طبعاً، أن يكون لديه برنامج كومبيوتر مماثل لما عند المرسل، وبالمفتاح ذاته. غير أن المنظومتين الآلية والرقميَّة، كانتا تضمّان عنصرين أساسيين، الأول ويدعى الصندوق الأسود والذي يحتوي قواعد التحويل، والثاني مفتاح يزود به الصندوق الأسود مع الرسائل اليومية الموضوعة بلغة عادية. وكانت تلك هي المعلومات الأساسيَّة التي كانت مدار حديث سيلفر في ذلك اليوم، ولكنه ولما كان غير مطّلع على أسرار الحكومة، فلم يكن يملك في الواقع إِلاَّ بعض التفاصيل. غير أنَّه كان، يستطيع أن يوضح كيف يمكن للكومبيوتر الذي يقوم بمعالجة منظومات التشفير أن يولد سلسلة من الأَرقام التي توفر دفقاً من المفاتيح للرسائل، ثم كيف تكون المزاوجة بينها وبين تيار من النصوص العادية للحصول على نص مشفّر. (تقوم هذه العمليَّة، كما يعرف أي عالم من علماء الكومبيوتر، على المزاوجة بين بت رقمي digital bit وآخر، وتوليد واحد أَو صفر حسب اتفاقهما أَو اختلافهما). وإذا كان المفتاح عصياً على الاكتشاف، فلسوف يكون نتاجك شريطاً من الثرثرة غير المفهومة، ولا يمكن حلّ رموزها (كما يأمل المرء) إِلاَّ باستخدام ذات المفتاح لعكس العمليَّة، وجعل النص واضحاً كما كان.

إن كلمة «عصي» هي، طبعاً، عبارة نسبيَّة، ولكن للتأكّد من «منعة» النّصّ، وضع أولئك الذين ابتكروا منظومات التشفير معياراً حرصوا عليه: العشوائية. والفكرة تقوم على ابتكار نصّ مشفّر يبدو أقرب ما يكون إلىٰ سلسلة من الحروف العشوائية، وإذا لم يكن الأمر كذلك، فإن أحد العاملين في تفكيك الرموز، يستطيع بما يتوفر له من الذكاء والدأب أن يتعامل مع أدقّ الأنماط ويعيد تركيبها كما وُضعت أصلاً. أما السلسلة المتدفقة من الأَرقام أو الحروف الموضوعة بصورة عشوائية تامّة، فحري بها أن توفّر للمرء شيفرة منيعة عصية على الحل، وهذا جوهرياً يمثّل أشدّ ما يمكن من أشكال التشفير منعة، ويُعرف باسم ورقة الحل لمرة واحدة one-time pad، وهو نظام يوفّر بديلاً موضوعاً بطريقة عشوائية حقاً لكل حرف في النص الواضح. ويعتبر الحل الوحيد الكريبتوجرافي الموثوق رياضياً بمنعته أمام محلّلي الشّيفرة.

غير أن المشكلة في ورقة الحلّ لمرة واحدة، هي أنك تحتاج لرقم مختلف ـ مقابل كل حرف في الرسالة ـ في مادة المفتاح الذي قام أصلاً بتحويل النَّصّ الواضح إلىٰ نصّ مشفّر. وبعبارة أخرى، لا بدّ أن يكون مفتاح الرسالة بطول الرسالة ذاتها، على الأقل، ولا يمكن استخدامه إلاَّ مرة واحدة وحسب. وقد جعلت صرامة العمليَّة تطبيقها أمراً صعباً من الناحية العمليَّة. وباءت بالفشل حتى المحاولات الجادّة لتعميمها، إذ أُحبطت جميعها من أولئك الذين حاولوا كسب الوقت وتوفير الجهد بتكرار استخدام مفتاح معين أكثر من مرة.

ولقد أثارت تلك الحوارات مع سيلفر اهتمام ديڤي وحماسته. وكان واضحاً مبلغ أهمية موضوع العشوائية الزائفة Pseudo-randomness للعالم الواقعي والرياضي، حيث يعتمد الأمن والسرِّيَّة على فعالية هذه الشيفرات. إلىٰ أي حد نستطيع أن نقترب من العشوائية؟ من الجلي أن هناك الكثير من العمل الذي يجري على قدم وساق لاكتشاف الإجابة عن هذا السؤال ـ ولكن هذا العمل كان يجري خلف حواجز منيعة أقامتها أَجهزة الاستخبارات الحكومية وتقوم على رعايتها.

والحق أن كل ما يتصل بالكريبتوجرافيا الحديثة وتفكيكها تقريباً، كان يجري خلف ذلك الحاجز. أما الآخرون جميعاً، فعليهم أن يعتمدوا على ذات النصوص التي تعرّف إليها هويتفيلد ديفي عندما كان في الصف الخامس الابتدائي. وهذه الكتب لم تمكن المرء من تغيير نظام تتابع الواحد والصفر في رسالة موضوعة بالكومبيوتر وتحويلها إِلىٰ مجموعة مختلفة من الأحاد، والأصفار الملتبسة تماماً عن طريق استخدام أحدث الآلات مثل المولدات من طراز فيبوناكي Fibonacci، أَو المسجلات الدورية، أَو المنطق اللاخطي للتغذية الراجعة. ولقد كره ديفي هذا، وخطر بباله أن «تقنية جيدة التطور تم الاحتفاظ بها سرّاً». وأخذ منه الغضب كل مأخذ لهذا العسف. وفي أحد الأيام، بينما كان يسير مع سيلفر في ماس أفنيو بالقرب من السكة الحديديَّة، أسرَّ له عن أسباب قلقه، بقوله: «إن الكريبتوجرافيا أمر حيوي لخصوصية الإِنسان وأسراره!» وأشار يومئذ إِلىٰ أنه كان على الباحثين ذوي الحمية في القطاع العام، أن يحاولوا إطلاق هذا الموضوع قائلاً: «لعلّنا نستطيع إن صممنا أن نكتشف من جديد، الكثير من تلك المادّة. وهذا يعني أن نتمكّن من نزع السرّيَّة عنها».

أما سيلفر فكانت الشكوك تراوده، فقال: «هناك عدد كبير من ذوي العقول الجبارة يعملون في إن إس أ NSA مشيراً بذلك إِلىٰ وكالة الأمن القومي National Security Agency حصن الكريبتوجرافيا لدى حكومة الولايات المتّحدة. ومضى سيلفر في شرح وجهة نظره بقوله إن هذه المؤسسة لا تضم بعض أفضل العقول في البلاد وحسب، بل لديها بلايين الدولارات أيضاً. ثم إن العاملينَ لديها يتمتعون بسنوات طويلة من الخبرة، ولديهم اطلاع تام على أحدث المكتشفات في هذا الحقل والأساليب التي يجهلها الناس العاديون ـ بالغاً ما بلغوا من الذكاء ـ ما لم يكونوا متمتعين بتصريحات أمنية عالية المستوى. وكانت الوكالة تحتفظ في الطابق الأرضي بحواسيب ضخمة ذات

قدرات عالية تتضاءل بجانبها الكومبيوترات المتطورة لدى معهد ماساتشوسيتس حتَّى لتبدو بالمقارنة بها أشبه بالآلات الحاسبة التي يحملها المرء في جيبه. فكيف يمكن لغرباء عن الوكالة، أمثال ديڤي وسيلفر أن يضارعوا وكالة الأَمن القومي؟

ولقد روى سيلفر لديڤي قصة عرضت له، وتتصل بوكالة الأَمن القومي، وذلك أثناء وضعه قبل سنوات مولد أرقام عشوائية لآلة بي دي بي ـ 1 PDP-1 التي كانت شركة ديجيتال إكويبمنت كوربوريشن [المعدات الرقميَّة] تقوم بصناعتها. وأنَّه قد احتاج لبعض المعلومات التي تتعلَّق بموضوع ليست له صلة بالكريبتوجرافيا، فكل ما هنالك أنّه كان بحاجة إِلىٰ بعض المعلومات الرياضيَّة عن عدد كثير الحدود ذي خصائص معينة. ولما كان واثقاً من أن صديقاً له يعمل في وكالة الأَمن القومي يعرف الجواب، فقد اتّصل به، فجاء جواب الصديق: «نعم، أعلم بالمسألة. ما هو العدد الذي تطلبه؟ ثم أعقب ذلك فترة من الصمت، وحسب سيلفر أن صديقه كان يطلب الإذن بالإجابة، ثم ردّ عليه ذلك العالم في وكالة الأَمن القومي بهمس المتآمر؛ «س إِلىٰ الخامس والعشرين، زائد س إِلىٰ السابع، زائد واحد».

ولقد ثارت ثائرة ديڤي لهذه السرِّيَّة. كان قد سمع الكثير عن وكالة الأَمن القومي، طبعاً، إِلاَّ أنه لم يكن يعرف الكثير عنها، وتساءل في خلده أي منظمة هذه التي تتصرّف وكأنَّها تمتلك حقائق الرياضيَّات؟».

كانت وكالة الأَمن القومي التي أمر الرئيس ترومان بإنشائها بقرار بالغ السرِّيَّة في خريف عام 1952، منظمة تبلغ ميزانيتها عدة مليارات من الدولارات، وتجري أعمالها كلها في المنطقة «السوداء» من الحكومة، حيث يقتصر حق المعرفة على أولئك الذين يقدمون البرهان على «حاجتهم للمعرفة» وحسب. (ظلت الوكالة مجهولة لا يدري بوجودها إِلاَّ قلّة مختارة حتَّى ورد اسمها بعد خمس سنوات من تأسيسها، في وثيقة حكومية؛ ولم تكن تعترف بوجودها قبل

ذلك الحين). كانت الوكالة ذات مهمة كريبتوجرافية مزدوجة: الحيلولة دون تسرّب المعلومات الحكومية، وجمع المعلومات عن الدول الأجنبية. وقد أدّت بطبيعتها المزدوجة، إِلىٰ تنظيم نفسها في قسمين رئيسيين: أمن الاتّصالات Communication Security ويعرف اختصاراً بـ COMSEC (كومسيك) ومهمته السعي إِلىٰ وضع شيفرات غير قابلة للتفكيك، وقسم رصد الاتّصالات Communication Intelligence أَو اختصاراً COMINT (كومنت) الذي يتولى جمع المعلومات من كافة أنحاء العالم، وتفكيك رموزها وتحليلها. (ولما كانت هذه العمليَّة تشتمل في الغالب على اعتراض وترجمة المعلومات المبثوثة إِلكترونياً فيشار إليها عموماً باسم مخابرات الإِشارة Signals Intelligence أَو SIGINT (سيجينت). ولقد أقامت وكالة الأَمن القومي على امتداد السنين شبكة واسعة من أَجهزة التنصّت، وأدوات الرصد لجمع الإِشارات السلكيَّة واللاسلكيَّة، وامتدت هذه الشبكة حتَّى أقاصي الكرة الأرضية، وبلغت مع بداية عصر الأقمار الصناعية في الستينات عالم الكواكب.

في مطلع السبعينات، لم يكن شيء من هذا موضع نقاش علني. وكان العارفون في هذا النطاق يشيرون إِلىٰ هذه المنظمة، على سبيل المزاح، بالوكالة التي لا وجود لها. وكان القلة القليلة من أعضاء الكونغرس الذين يتولّون مسؤوليَّة تمويل وكالات الاستخبارات، لا تبلغهم المعلومات عنها إِلاً داخل الغرف المغلقة، بعد تفتيشها بدقَّة خشية وجود أَجهزة تنصّت فيها.

وكان الدخول إِلىٰ مقر المنظَّمة في فورت جورج ميد، بولاية ماريلاند، كما يمكن للمرء أن يتوقع، مقصوراً على عدد محدود جداً من الأفراد، وكان المقر محاطاً بسياج من ثلاثة أطواق مكهربة لردع الغرباء من الاقتراب. أما العمل في الداخل، فكان يخضع للتدقيق الشديد.

ويطالع المرء في مقدمة الدليل، الذي يقدّم للعاملين الجدد العبارات التالية: «إن انضمامك إِلىٰ وكالة الأَمن القومي، يمنحك فرصة للمشاركة في

نشاطات إحدى أهم وكالات الاستخبارات في حكومة الولايات المتّحدة، ويدل ذلك على أنَّك قد حزت على الثقة التي تؤهلك لحمل مسؤولية من أضخم المسؤوليّات التي ينهض بها فرد من الأفراد، مسؤولية الحفاظ على معلومات بالغة الأهمية لأمن شعبنا.

ولما كانت كافَّة المعلومات الهامَّة المتّصلة بالكتابة السرِّيَّة يحظر اطلاع الجمهور عليها، فليس بوسع الغرباء عن الوكالة إِلاَّ تخمين ما يجري داخل «القلعة». ومما لا ريب فيه، أن الوكالة كانت تقوم بأشد عمليات الاستطلاع والتجسّس تعقيداً في العالم. وكان الاعتقاد السائد (وإن لم يكن ثمة اعتراف بذلك) أنَّه ما من مكالمة هاتفيَّة أَو نشرة إخباريَّة أَو برقية تُرسل في بلد أجنبي بمأمن من أَجهزة الرصد التي تديرها الوكالة وكأنَّها مكنسة كهربائية على مستوى الكرة الأرضية، تلتقط الإشارات التي يصار إِلىٰ تحليل محتوياتها باستخدام كومبيوترات إم آي بي إس MIPS [لها القدرة على التعامل مع مليون أمر في الثانية. هـ. م] المتعدِّدة المستويات التي تقوم بتمشيط النص بحثاً عن أي أمر ذي قيمة. (وقد تأكدت هذه الشكوك فيما بعد مع تسرّب المعلومات عن مشروع النسق Project Echelon، ذلك البرنامج الطموح الذي وضعته الوكالة لرصد الاتّصالات الخارجيَّة). فهل كانت نتائج المشروع تتناسب مع مليارات الدولارات التي صُرفت، والأخلاقيَّات المشكوك فيها لتلك الجهود ذاتها؟ إن معرفة ذلك أمر لا يحيط به إِلاَّ قلّة محدودة جداً من المسؤولين في الحكومة الذين يتلقّون مذكرات موجزة عما تحصل عليه أجهزة الرصد الخرافية هذه ـ بل إن نوع المعلومات يعتمد على ما تقدّمه لهم الوكالة ذاتها.

والأدهى من ذلك، أن وكالة الأَمن القومي تعتبر نفسها المستودع الوحيد للمعلومات الكريبتوجرافية في البلاد، ولا يقتصر ذلك على تلك المعلومات التي تفيد منها الحكومة المدنية والقوَّات المسلَّحة بكافة صنوفها، كما يقضي القانون، بل تلك التي يستخدمها القطاع الخاص أيضاً. وإذن، فليس السياج

المكهرب الذي يحيط بمقر الوكالة بأطواقه الثلاثة حاجزاً مادياً وحسب، بل هو رمز لسعي الوكالة الذي يبلغ حدّ الهوس لإخفاء المعلومات حول نفسها ونشاطاتها أيضاً. ليس ثمة في الولايات المتّحدة الأمريكية شيفرة أَو كتابة سرِّيَّة ذات شأن، إلاّ ما يوجد وراء «السياج الثلاثي».

تقوم وكالة الأَمن القومي كل يوم بدراسة أفكار جديدة لمنظومات كريبتوجرافية يقدِّمها المبتكرون في هذا الحقل. وفي هذا كتب ديڤيد كاهن: «إن أفكار هؤلاء المبتكرين، تختفي في جوف وكالة الأَمن القومي المظلم، ثم قد توظّف في الكريبتوجرافيا الأمريكيَّة، غير أن الجانب الأمني يحول دون معرفة المبتكر بهذا، وقد يسمح للوكالة أَو موظفيها، استخدام أفكاره دون تعويض له». ومع ذلك، حتَّى الذين لم يقدِّموا أفكاراً ليسوا بمنجاة من قبضة الوكالة القوية. فالوكالة تقوم بتمحيص كل طلبات تسجيل الملكية الفكرية ذي صلة بالكريبتوجرافيا، وتتمتع بسلطة قانونية تتيح لها حظر تداول أي ابتكار ترى أنَّه قد يشكِّل خطراً إن أصبح في متناول الجمهور.

ومع ازدياد اطلاع هويت ديڤي على ما يتصل بوكالة الأَمن القومي، غدا يشعر في دخيلته بشيء من الحماقة، لأنه وإن كان قد علم بوجودها، فإنه لم يدرك مدى سلطانها إلاّ مؤخراً. وكان ديڤي قد سبق له أن زار فعلاً معهد تحليل الشؤون الدفاعيَّة في جامعة برنستون، وهو منشأة شبه خاصة، ومركز متقدِّم لوكالة الأَمن القومي، ولكن لم تكن لديه يومذاك سوى فكرة غامضة عن مهمة المنظمة. ولا يعني ذلك أنَّه كان يمكن له الحصول على المعلومات من جهابذة الشّيفرة. فقد يخالط المرء أولئك الذين يقبعون وراء السياج الثلاثي، بل ربما تبادل وإياهم الأفكار أيضاً، لكن شريطة ألا تمس موضوع الكريبتوجرافيا، المحرم.

غير أن الكريبتوجرافيا هي بالضبط الموضوع الذي كان ديڤي يرغب بالخوض فيه. فقد كان يود الحصول على أقصى ما يمكنه من المعرفة بهذا

الموضوع، وأن يجري الأحاديث المعمّقة مع القادة الكبار في هذا الميدان. بل كان يقبل حتّى بالحديث مع «الجنود المشاة» في هذا المجال. ولكن سرعان ما أصبح محبطاً بسبب أولئك الذين كانوا يتجنّبون الخوض في هذا الموضوع، أو ما كان باستطاعتهم التطرّق إليه.

ومن ذلك، أن ديفي حينما سأل أحد زملائه في معهد ماساتشوسيتس للتكنولوجيا، ويدعى دان إدواردز، والذي كان سيعمل في وكالة الأَمن القومي بعد تخرّجه. والذي وصفه ديفي فيما بعد بقوله: «كان غير متعاون إلىٰ أقصى حدّ، ولم يكشف (لي) عن أمور لم تكن قطعاً من الأسرار، وقد وقعت عليها فيما بعد بين المراجع التي اعتمد عليها في أطروحته». وعندما انضم أحد زملائه في شركة ميتري إلىٰ مؤسّسة تحليل الشؤون الدفاعيَّة، سأله ديفي إن كان يستطيع أن يفيده بشيء عن عمله، فأجابه الزميل القديم بعد فترة من الصمت المثير: «لا».

ولربما كانت فكرة معرفة المحظور أقوى من أن يقاومها مشاكس، عنيد مثل ديفي. فقد ظلت الكريبتوجرافيا والخطر الصامت على الخوض في موضوعها يشغلان فكره. وكان كلما ازداد انشغالاً بالمشكلة، ازداد إدراكاً لمبلغ أهمية الموضوع، وخاصة في ما رأى أنّه عصر الحوسبة القادم. وقد وجد أن طلب الناس للكريبتوجرافيا سيزداد مع ازدياد استخدامهم للكومبيوتر، والهواتف اللاسلكيَّة، وسوى ذلك من الأَجهزة الإِلكترونية. فكما أن اختراع التلغراف ساعد في الإقبال على الكريبتوجرافيا بنقل الرَّسائل عبر آلاف الأميال دون قيود، مما وفَّر فرصة ممتازة ليمارس المتنصّتون من كل حدب وصوب عملهم، كذلك سيكون من شأن عصر الكومبيوتر أن ينقل مليارات الرسائل التي كانت تدوّن على الورق، فيجعلها تجري في مملكة البتات Bits. وإذا كانت هذه دون تشفير، فإن ذلك يجعلها ثماراً يانعة، لمن شاء قطافها من المتطفلين. فهل نجد في الكريبتوجرافيا، هذا العلم الذي تعمّدت قوى الحكومة إحاطته بظلام

السرّيّة، ما يساعد على إفشال مسعى المتطفلين؟ وقد جاء الجواب جلياً كالنص الواضح. طبعاً، تستطيع الكريبتوجرافيا أن تساعد في هذا الأمر.

كان في معهد ماساتشوسيتس للتكنولوجيا مثال ممتاز عن الحاجة إلىٰ حل كريبتوجرافي لمعضلة كبرى. ذلك أن جهاز الكومبيوتر الرئيسي هناك، وكان يسمى «نظام المشاركة الزمنية المتوافقة Compatible Time Sharing System (أو اختصاراً سي تي إس إس CTSS) وهو أحد أوائل الحواسيب التي تَستخدم المشاركة الزمنية، ذلك التدبير الذي يتيح لعدة مستخدمين العمل على الكومبيوتر في آن واحد. وكان الاشتراك في استخدامه يتطلّب بعض الاتفاقيات لحماية المعلومات التي تخص كل طرف، والحيلولة دون اطلاع الشركاء الآخرين عليها. فكان الحل في هذا النظام بتخصيص كل من يستخدم الكومبيوتر بكلمة سر تكون مفتاحاً له، وبذلك تكون الملفات أشبه بمستودع صغير مغلق يختزن المعلومات، وكل كلمة سرّ بمثابة مفتاح للباب الموصل إلىٰ ذلك المخزن. والمسؤول عن توزيع كلمات السر، والاحتفاظ بها، إنما كان إنساناً هو مشغل النظام. وهذه الشخصية المركزيَّة تهيمن في الحقيقة على أسرار كل مستخدِم. وحتّى لو كان هذا الشخص أميناً شديد الحرص على حماية كلمات السر من التسرّب، فإن وجودها في نطاق نظام مركزي يسمح في حد ذاته بالمجازفة بسريتها. ففي وسع السلطات خارج هذا النطاق، امتلاك هذه المعلومات السرِّيّة، إذ يكفي أن تطلب السلطات من مشغّل النّظام ما تريد معرفته، حتّى «يرتكب ذلك الشخص خيانة بحقك، إذ لا مصلحة له في تحدي الأمر الصادر إليه، والتعرّض للسجن ليصون معلومات تخصّك أنت»، كما يقول ديفي.

كان ديفي يأخذ بما يصفه بـ «النظرة اللامركزية للسلطة»، وقد ذهب به الاعتقاد، إلىٰ أنّك تستطيع حل المشكلة، بإيجاد الأدوات الكريبتوجرافية المناسبة ـ عن طريق نقل مسؤوليَّة حماية البيانات من طرف ثالث لا مبالٍ بالمستخدِم الفعلي، أي الطرف الذي تتعرَّض أسراره الخاصَّة للخطر، وكان

يراود خياله إنشاء شركة تقوم بإنتاج مثل هذه الأدوات واستخدامها. بل لقد غدت هذه الشركة المتخيلة، أقرب إلىٰ الحقيقة الماثلة، حتَّى أنَّه أطلق عليها اسماً: شركة حماية السرِّيَّة.

إلاَّ أن صاحب الحلّ ومؤسِّس الشركة، كان في مخيلة ديڤي شخصاً آخر وليس ديڤي نفسه. فمع أنَّه أصبح متيقناً من أن مشكلات المحافظة على السرِّيَّة في عالم تُنتهك فيه الأسرار، لا يمكن تذليلها، فقد افترض أن الآخرين يبزونه من حيث التأهيل والاندفاع والنزعة العمليَّة، وأقدر منه على ابتكار الكريبتوجرافيا التي تتصدَّى لتلك المشكلات. ولذلك حاول إقناع الآخرين بالعمل على إيجاد هذا الحل لكن دون نجاح يُذكر، وفي هذا يستذكر: «لم أجد أحداً ممن حاولت إثارة اهتمامهم بالموضوع، يأتي بأمر في هذا الاتجاه».

وهكذا ثابر ديڤي على العمل في مجال اهتمامه الأساسي وهو معضلة رياضيَّة تسمّى «برهان الصحة» Proof of Correctness. غير أنَّه ظلّ يبحث قدر المستطاع، في موضوع الكتابة السرِّيَّة والشّيفرة، وإن كانت جهوده حتَّى هذه اللحظة، بعيدة عن العمل المنهجي. وفي أحد الأيام، وبينما كان يستطلع الكتب الوارِدة حديثاً إلىٰ المكتبة العامّة في كمبردج، وقع على كتاب The Broken Seal (الخاتم المكسور) للا ديسلاس فاراجو، ويتناول الجهود المبذولة لفكّ الشّيفرة، حتَّى ما قبل الهجوم على بيرل هاربر. وأخذ يتصفح الكتاب فوجده جديراً بالقراءة حقاً. إلاَّ أنَّه لم يقم بذلك على الإطلاق. (والأسوأ من ذلك أنَّه خلط بينه وبين كتاب آخر صدر في ذلك الحين، وهو كتاب The Code Breakers (مفكّكو الشّيفرة) لديڤيد كاهن، مما أدَّى إلىٰ تأخير قراءته لذلك الكتاب الأكثر أهمية).

ومن المصادفات أيضاً أن زميلاً له أعطاه، وهو يغادر مكتبه في شركة ميتري، نسخة من بحث وضعه عام 1949 كلود شانون أبو نظرية المعلوماتية الأسطوري، والذي كان يدرس في معهد ماساتشوسيتس منذ عام 1956، إلاَّ أن

ديفي لم يلتق بالأستاذ الضئيل الجسم، والانطوائي، والذي يعيش حياة عائلية هادئة، وتشغله اهتماماته المتعددة، بدءاً من مطالعة قصص الخيال العلمي حتَّى سماع موسيقى الجاز. (وكان ماهراً في ركوب الدراجة ذات العجلة الواحدة، حتَّى انقطع عنها على ما يظن في الستينات من عمره).

كان تأثير شانون على الكريبتوجرافيا عظيماً. فبعد نيل شهادة الدكتوراه من معهد ماساتشوسيتس للتكنولوجيا (أم آي تي) عام 1940، عمل أثناء الحرب في مخابر شركة بيل للهاتف، واختص في عمله بالمنظومات السرِّيَّة. وكان العمل آنذاك من الأسرار، طبعاً، ومع ذلك فقد وجدت دراستان هامَّتان وضعهما شانون أثناء الحرب طريقهما إِلىٰ النشر، وأصبحتا من الأعمال المتاحة لإطلاع الجمهور. ففي عام 1948 نشر مقاله الرائد في المعلوماتية «نظرية رياضية في الاتِّصالات» في مجلة بيل سيستم تيكنيكال جورنال Bell System Technical Journal، وأعد المسرح لبداية العصر الرقمي digital. ثم ظهر بعد عام مقاله «نظرية الاتِّصالات في المنظومات السرِّيَّة» في المجلة ذاتها.

كان المقالان كلاهما موغلين في التخصّص، وما كان بوسع القارئ غير الحائز على شهادات عالية في الرياضيَّات أن يمضي في قراءة أكثر من بضع فقرات، إذ سيجد نفسه وسط دغل من المعادلات والصِّيغ الشائكة. غير أن شانون كان يتمتع بميل للوضوح، أتاح له أن يرسل إشارة جلية وسط ضجيج من الرياضيات العالية المستوى. وقد تجلى ذلك في البحث الثاني، حيث استعرض بوضوح واختصار العلاقات الكريبتوجرافية الأساسيَّة من البداية، وتناول «البنية الرياضيَّة العامَّة وخصائص المنظومات السرِّيَّة». وقدّم فوق ذلك رسماً تفصيليّاً لوضع كلاسيكي في تحليل الشّيفرة، يبدأ بصورة صندوق، يمثِّل الرسالة الأصلية التي يحولها مشفِّر encipherer، إِلىٰ رسالة مشفَّرة استناداً إِلىٰ «المفتاح المصدر»، وبموجب هذا المخطط تنتقل الرسالة المشفَّرة إِلىٰ من يقوم بفكّها decipherer باستخدام المفتاح المصدر ذاته لإعادتها إِلىٰ حالتها الأصلية.

غير أن ثمة خطأً آخر يتفرع عن الرسالة المشفَّرة Cryptogram، يؤدي إلىٰ محلِّل الشّيفرة المعادي الذي يتمكّن من اعتراض الرسالة المشفرة. وكان لا بد من افتراض وجود طرف ثالث على الدوام. فالتحدي يتمثَّل في الحيلولة دون تمكين العدو من فك النص المشفّر.

كان لمفهومي «الإِشارة» Signal و«الضجيج» noise المكانة الكبرى في نظرة شانون إلىٰ الكريبتوجرافي (علم الشيفرة). فقد كان يرى في الشّيفرة لعبة عالية المجازفة، ومحصلتها صفر تدور بين حارس السر وخصم، حيث السر الذي ننجح في إبقائه سراً، هو إشارة يستحيل استخلاصها وسط الضجيج الظاهر. وقد بسط شانون المسألة ببراعة، في ستين صفحة، وأوضح المعضلة التي تواجه كلاً من واضع الشّيفرة والعدو. ولا ريب بأن تلك الهدية التي تجلت في مقال شانون، كانت من أثمن ما يمكن لواضع شيفرة في المستقبل، مثل ديفي، أن يأمل بالحصول عليها في أواخر الستينات. وقد وصف ديفي فيما بعد بحث شانون بأنَّه آخر بحث ثمين غير محظور، يصدر في ما يزيد عن عشرين عاماً.

وإنه لأمر يدعو للأسف أن يكون هويت ديفي قد انتظر، وهو في سعيه غير المنتظم إلىٰ المعرفة، عدَّة سنوات قبل أن يلتفت لقراءة هذا البحث.

في عام 1969 ترك ديفي العمل في شركة ميتري. وكان ما لديه من مال قد نفذ، وبات قريباً من السنّ الذي يتجاوز فيه الخدمة الإلزاميّة، وبذلك توفّرت له حرّيّة ترك العمل. والحق أَن كمبردج لم تستهوه. فقد أَلِف في أيام الدراسة صحبة اليساريين الليبراليين، بل الحمر كذلك. وعاش حياة اجتماعية غنية، واعتاد ارتياد حفلات الغناء الشعبي، وكانت له صداقات كثيرة مع فتيات ودودات. ولا ريب أن مثل هذه الأحوال كانت معروفة في كمبردج، لكن ديفي كان في شاغل عنها، إذ يقول اليوم بشيء من الحسرة: «إنني ببساطة لم أصادف هناك وضعاً شبيهاً بذاك». أما في جامعة كاليفورنيا في بيركلي حيث أمضى فصل

الصيف بعد السنة الجامعية الأولى، فقد وجد لنفسه مكاناً بين حشد الطلبة اليساريين المعارضين. ويصف حاله آنذاك بقوله: «إنني مؤمن بوجهة النظر الراديكاليَّة، ولطالما كنت أؤمن بأن معتقدات المرء السياسيَّة وطبيعة عمله متلازمين، ولا يمكن الفصل بينهما».

انتقل ديفي وصديقته إِلىٰ الغرب، ومضى للعمل في مختبر الذكاء الاصطناعي في جامعة ستانفورد الذي كان يديره جون مكارثي. وكان يفترض به يومذاك أن يتابع البحث في برهان الصحّة ومعضلات رياضيَّة أُخرى تتَّصل بعلم الكومبيوتر. لكن ديفي وجد نفسه ينساق، أثناء أحاديثه مع مكارثي، للانشغال بالمسألة الأعمق: المتصلة بالسرِّيَّة والخصوصيَّة. فقد أدرك مكارثي، وهو رائد في المشاركة الزمنية في الكومبيوتر، أن الحواسيب ستدخل البيوت في وقت قريب، ولا بدّ بالتالي، في اعتقاده، من أن يصيب التغيير طبيعة العمل ذاته، عندما يخرج المكتب الإِلكتروني من عالم علماء الكومبيوتر والمتسللين المغلق، ليصبح أداة شائعة. ولن يؤدي هذا إِلىٰ إثارة مجموعة من المعضلات الأمنية فحسب، وإنما سيطرح جملة متداخلة من التحديات الجديدة، ما كانت لتخطر ببال أحد عام 1969. ومن ذلك التساؤل: كيف يمكن للناس نسخ استمارات التوثيق المألوفة (وهي وسيلة إثبات شخصية صاحب الوثيقة) إذا غدا نتاج العمل إِلكترونياً، ينتج بالكومبيوتر ويرسل عبر شبكات رقميَّة؟ ثم كيف تستطيع الحصول على معادل موضوع بالكومبيوتر لعقد موقع؟ فحتَّى لو أعطي الناس «تواقيع رقميَّة» فريدة ـ لنقل رقماً عشوائياً طويلاً لشخص بمفرده ـ فإن طبيعة الوسيلة الرقميَّة التي يمكن بها نسخ ما شئت بأجزاء الثانية، يبدو أنَّها تجعل مثل هذا المعروف موضوعاً لا طائل منه. فإذا وقعت عقداً بهكذا رقم، فما الذي يحول، عندئذ، دون قيام شخص ما، بانتحال التوقيع وتقديم نسخة كاملة من العقد، وربطها بوثائق وعقود وشيكات مصرفية أخرى؟ إن مجرد احتمال وجود مثل هذه النسخ المنحولة، سيجعل التوقيع دونما قيمة. وقد

ينبري من يقول: «إنني لم أوقّع مثل هذه الأوراق. إن أحدهم قد نسخ توقيعي». وأخذ ديفي يتساءل في خلده: كيف يمكن للمرء أن يتبيَّن هذا الخلل الأصيل في مفهوم التجارة الرقميَّة؟

ولقد أمضى ديفي ومكارثي ساعات في مناقشات مستفيضة، في قضايا مثل التحقّق من صحة الرسائل الصادرة، والقضايا المتصلة بتوزيع المفاتيح الإلكترونية. ولكن كان ديفي لا يزال يؤثر دفع سواه لحل المعضلات. غير أن المكائد في العاصمة واشنطن دفعت بالأمور في صيف عام 1972، بطريقة غير مباشرة إِلىٰ تغيير هذا المنحى.

كانت الحكومة برعاية من وكالة المشاريع والأبحاث المتقدمة Advanced Research Project Agency (اختصاراً ARPA أربا) التابعة لوزارة الدفاع، قد أخذت حديثاً ببرنامج يصل بين مؤسَّسات البحث الرئيسة. وعرف هذا البرنامج باسم أربانت Arpanet [شبكة وكالة المشاريع والأبحاث المتقدمة] وهو نظام قُدِّر له أن يتحوَّل إِلىٰ ما يعرف اليوم بالإِنترنت. وقد أدرك لاري روبرتس، مدير قسم تقنيات معالجة المعلومات في أربانت، أن مثل هذه الشبكة من الكومبيوتر، وهي أول شبكة تصل بين عدة مواقع، وتقوم بخدمة المئات، إن لم يكن الآلاف من مستخدميها، سوف تكون بحاجة إِلىٰ طريقة توفر أمن الرسائل، والطريقة الجلية لذلك هي إيجاد حلول كريبتوجرافية جديدة. ولكن حين التمس المساعدة من وكالة الأمن القومي صُرف من هناك على عجل. وفي النهاية طلب روبرتس المساعدة من شركة بولت بارانيك نيومان في بوسطن التي ساهمت في إقامة أربانت أصلاً. وكان في نفس الوقت قد عرض المشكلة على صديقه جون مكارثي الذي كان يشجع القوم في ستانفورد على وضع بعض البرامج في الكريبتوجرافيا. فأخذ هؤلاء في العمل على ما وصفه ديفي فيما بعد بـ: «نظام بالغ التعقيد» يجمع بين تأثير عدة مولدات أرقام عشوائية خطية متناسقة».

وقد وجد ديفي نفسه ينضم إِلىٰ هذا المجهود، بسبب وجود صديقته بين

أفراد الفريق. وكان أن قاده فضوله، بطبيعة الحال، إِلىٰ دراسة هذا النظام بعناية. ولما استوعب مادته، وجد نفسه تضيق به لافتقاره للكفاءة. فقد كان ديفي يعتقد بأنه إذا ما تم استخدام الكريبتوجرافيا في الكومبيوتر، فمن الضروري ألا يعاني مستخدمو الكومبيوتر من بطء في الأداء. وكان الرأي عنده أن التشفير، في الوضع المثالي، ينبغي ألا يكبد المستخدِم إِلاَّ بعض الوقت، وبمقدار لا يلحظ، في أداء وظيفة مثل نسخ ملف. وشرع ديفي يراجع خوارزمية الشّيفرة الأساسيَّة التي تأخذ بها المجموعة وقام بوضع منهج أسرع كثيراً من الذي يعملون به. وإذ انغمس الرجل في العملية وبات ينشغل بوضع بعض الشّيفرات، راح يولي المزيد من الوقت للتفكير في القضايا الأوسع، وهي تطوير هذا الحقل. وبعد فترة من ذلك العام ذهب إِلىٰ كمبردج، وقابل رولند سيلفر من جديد، وقد غدا ديفي الآن أكثر خبرة ليغني بها موضوع الشّيفرة؛ كما غذت أحاديثهما الغنية اهتمامه بالموضوع وزادت من انشغاله به.

وفي ذلك الوقت، أتيح لديفي قراءة كتاب ديفيد كاهن «مفكّكو» الشّيفرة. وكانت قراءة هذا الكتاب الضخم الذي تبلغ صفحاته الألف، مهمّة كبرى لديفي، وهو القارئ المتأنّي والمدقّق. وتقول صديقته هارييت فيل: «كان يصطحب الكتاب معه أينما حل أَو رحل. فإذا دعوته إِلىٰ العشاء جاء والكتاب في يده. لكن ديفي وجد في مئات الساعات التي أمضاها في قراءة هذا الكتاب أحسن استثمار».

والحق، أن كتاب «مفكّكو الشّيفرة» كان معلماً في مجاله، كتاباً ما كانت الحكومة تريد له أن يُنشر. وكان مؤلفه كاهن مراسلاً لصحيفة نيوزدي News day، وقد آفتتن منذ أن كان في الثانية عشرة من عمره، شأنه شأن ديفي ومن لا عد له ولا حصر من الفتيان، حين تعرّف لأول مرة إِلىٰ ألغاز الكتابة السرِّيَّة. وكانت تلك اللحظة، يوم زار المكتبة العامّة في بلدة جريت نك (لونغ إيلند، بولاية نيويورك)، حيث وجد في لوحة عرض الكتب غلاف كتاب مشوق في

التاريخ بعنوان: سري وفوري Secret and Urgetn لفليتشر برات. ويستذكر كاهن الآن تلك اللحظة قائلاً: «كان ذلك في عام 1942 أَو 1943. وكان غلاف الكتاب رائعاً، وعليه صورة أرقام وحروف تبرز من الكون في حركة كالدوامة. ووجدتني يومئذ مسحوراً بما رأيت». ولقد ازداد افتتاناً بالكتاب حين طالع ما فيه، وعلم كيف تعمل الشّيفرة. وحمله ذلك التأثّر على الانتساب إِلىٰ أرقى منظمة غير حكومية تُعنى بالكريبتوجرافيا، هي جمعية الكريبتوجرام (النص المشفّر) الأمريكية. وكانت جمعية بسيطة العدة، «حفنة من الهواة يعملون في حلّ النصوص المشفّرة كألغاز، وينشرون مطبوعة متواضعة يكتبون فيها مقالات حول كيفية إيجاد الحلول». كما يذكر كاهن. وكان الكثير من أعضاء الجمعية من كبار السن، أَو كان لديهم، على الأقل، متسع من الوقت للانشغال بالألغاز وحلّها، بل كانت هناك أيضاً جماعة متفرعة عن الجمعية يعرفون باسم ملازمي الفراش، «وهؤلاء كانوا من المصابين بشلل الأطفال، أَو مرضى مقيمين في ما يشبه المصحة، أَو يعانون من الشلل. وما كان بوسعهم الحركة، فآثروا الانشغال بحلّ الألغاز». كما يقول كاهن. ذلكم هو مقدار العمل في الكتابة بالشّيفرة خارج إطار الحكومة.

كان كاهن، على كل حال، شغوفاً بحل الألغاز، على العكس من ديفي، وظلّ على اهتمامه هذا حتّى بلغ مبلغ الرجال. كذلك كانت له جولات في مناقشة بعض المخطّطات المعقّدة مع زملائه في الجمعيّة. وفي ذلك يقول: «لولا تلك المناقشات، لوجدت نفسك في عزلة تامّة. فقد كان هذا حقلاً مجهولاً، وليس ثمّة من له معرفة به». ولم يلحظ كاهن وجود اهتمام عام بالكريبتوجرافيا حتّى عام 1961 حين هرب اثنان من المختصين به يعملان لدى وكالة الأَمن القومي إِلىٰ الاتحاد السوفييتي، وعقدا مؤتمراً صحفياً عرضا فيه تجربتهما. وقد كان ذلك الحدث بمثابة كشف لكاهن؛ ذلك أنّه بالرغم من دأبه على رصد كل ما يصدر من المطبوعات المتاحة للنّاس في مجال

الكريبتوجرافيا، إلاّ أنه لم يكن يعلم بوجود وكالة الأَمن القومي حتّى تلك اللحظة! ومع ذلك، فإن إلمامه بشيء عن الشّيفرة، حمله على الاتّصال بالمحررين في مجلة نيويورك تايمز لسؤالهم إن كانوا ينشدون من يوفّر لهم شيئاً من المعرفة عن أصول الموضوع. فردّوا بالإيجاب وقام هو بذلك.

وكان من أثر ذلك، أنّه تلقّى في اليوم التالي لظهور مقاله ثلاثة عروض لوضع كتاب حول هذا الموضوع. لكنّه رفض تلك العروض لأنّها تتضمّن ظهور الكتاب في طبعة شعبية، ويريد لكتابه أن يصدر في طبعة فاخرة. ثم تحقّقت رغبته بعد أسبوع، حين اتصل به محرّر يدعى بيتر ريتز طالباً وضع كتاب ليصدر في طبعة فاخرة عن الناشر ماكميلان. فقام كاهن بوضع مخطط لكتاب عام عن الشّيفرة، وتلقّى سلفة بمبلغ ألفي دولار. ولكن ما أن شرع في العمل على الجزء التمهيدي حتّى تجمعت لديه بفضل جهوده في البحث، قصص أشد طرافة مما كان قد حسب، وأخذت تتراكم لديه من مختلف المصادر، وما إن بلغ الصفحة 250 من فصل التمهيد ـ ولعله لم يكن وصل بعد إلىٰ عصر النهضة ـ حتّى أدرك أنّه كان في الحقيقة يكتب التاريخ الموسّع للكريبتوجرافي (علم الشّيفرة).

كان كاهن قد أمضى حتّى ذلك الحين، سنتين من العمل في هذا المشروع، فآثر أن يستقيل من عمله ليكرّس جهوده كاملة لإنجاز الكتاب. وأخذ ينفق من مدخراته، ويعيش في بيت والديه، ويأكل مما تطهوه جدته. وقد كتب في تلك الفترة مئات الرسائل، وكان يمضي أيامه في المكتبة العامة بنيويورك، والأهم من ذلك أنّه أخذ يتّصل بأناس لم يسبق لهم أن رووا تجاربهم. وقد أتاح له مسؤول رفيع في وزارة الدفاع الاتّصال باثنين من العاملين الهامّين في فكّ الشّيفرة إبان الحرب العالمية الثانية، وذلك أمر يدعو للدهشة، إذا ما أخذنا بالاعتبار ما نصّت عليه سياسة الحرب الباردة من أن الكشف عن أي معلومات، هو ضرب من الخيانة تقريباً، إذا ما قبل بتقديم مدوناته عن تلك اللقاءات إلىٰ

الحكومة. وكان تقدير كاهن، كما عبّر عنه: «أحسب أن [المسؤول في وزارة الدفاع] لم يكن يدري حقيقة ما تورّط به، فقد أصيبت الحكومة بالذعر حين سُلمت المدونات إِلىٰ وكالة الأَمن القومي، وقال لي [هذا المسؤول] إن عليّ [أن أتجاهل هذه المعلومات]. ولقد رفضت الطلب مع وافر الاحترام».

كذلك قدَّم كاهن، بمعونة من مصدر سريٍ موثوق وهام، أول رواية من خارج الإطار الحكومي عن مبلغ سلطة وكالة الأَمن القومي، جامعاً أطرافها من قطع وأجزاء توفرت له عبر السنين. لكن أشد التفاصيل خطورة في كتاب كاهن، إنما كان الشرح المنهجي لكيفية عملِ الكريبتوجرافيا وكيفيَّة استخدام الوكالة لها. فلما انتهى العمل في كتاب «مفكِّكو الشّيفرة» سنة 1965، وجدناه يضم أكمل وصف للعمليات التي تجري في مقر الوكالة، في فورت ميد، دون أن يحمل عبارة سرِّي للغاية على كل صفحة.

ولقد أصيب المسؤولون في وكالة الأَمن القومي بالذهول، حين اعتبروا كتاب كاهن قنبلة يدوية في شكل كتاب، وذا ضرر بالغ لسور السرِّيَّة الذي أحكمت الحكومة بناءه. وفي هذا الصدد كتب جيمس بامفورد مؤلِّف كتاب قصر الألغاز The Puzzle Palace الذي يكشف فيه أسرار وكالة الأَمن القومي: «لقد صرفت ساعات لا حصر لها في اجتماعات ومناقشات ضمّت أعلى المستويات من المسؤوليِّن في الوكالة، ومن بينهم المدير، في محاولة لتطويق الكتاب». وتراوحت الإجراءات المضادة التي درست خلف السياج الثلاثي، ما بين إمكانية شراء حقوق الطبع، إِلىٰ اقتحام بيت كاهن ذاته. وتم وضع كاهن، الذي كان قد انتقل إِلىٰ باريس للعمل في صحيفة «الهيرالد تريبيون»، على قائمة «المراقبين» في وكالة الأَمن القومي، مما يسمح للراصدين بقراءة بريده والتنصّت على مكالماته الهاتفيَّة.

شعر كاهن بالفزع، حين أرسل محرّر الكتاب في آذار/ مارس 1966، المخطوط إِلىٰ البنتاغون لقراءته والتعليق عليه. وكان المخطوط قد أرسل طبعاً،

إِلىٰ فورت ميد. وكتبت وزارة الدفاع إِلىٰ رئيس مجلس إِدارة دار ماكميلان أن نشر كتاب «مفكِّكو الشّيفرة» «لن يفيد المصلحة الوطنية». لكن الدار لم ترضخ، ليس بسبب مبادئها، حسب تقدير كاهن، بل لخشية الإِدارة من خسارة «المبالغ الضخمة التي استنفذها الكتاب»، وهو على وشك دخول عملية الإنتاج.

وهذا ما جعل الوكالة تقدم على خطوة خارقة، ففي تموز/ يوليو قام مديرها: الفريق مارشال إس كارتر ـ وكان رجلاً بلغ به نزوعه إِلىٰ السرِّيَّة ما جعل اسمه لا يرد في أي صحيفة على الإطلاق ـ بالسفر بالطائرة إِلىٰ نيويورك والتقى رئيس مجلس إِدارة دار النشر، ومستشارها القانوني، ومحرِّر كتاب كاهن، بيتر ريتنر. وبعد أن قام كارتر يومذاك بالطعن في سمعة كاهن وخبرته، ناشدهم في النهاية أَن يحذفوا ثلاثة أمور محدّدة. وبعد أيام من ذلك الاجتماع قدّم ريتنر الطلب ذاته إِلىٰ كاهن لنيل موافقته. ولقد استغرب كاهن المواقع المطلوب حذفها، إذ بدت له غير ذات شأن، وفي ذلك يقول: «لم يكن الحذف ليسيء إِلىٰ الكتاب حقاً، فقمت بحذف المواقع الثلاثة منه. لكنني ألحيّت على نشر بيان يفيد بأن الكتاب قد عُرض على وزارة الدفاع. وكان لذلك في النهاية تأثير حسن، إذ لم يعد لمراجعي الكتب اليمينيين حجة للادعاء بأن الكتاب مدمِّر للجمهورية. فهذا لم يعد بالذريعة الممكنة».

ومع أن الكتاب لم يكن في قائمة «نيويورك تايمز» للكتب الأكثر رواجاً، إلاَّ أنه حظي بإقبال دائم، حتَّى بلغت إصداراته أكثر من عشر طبعات. كما أنَّه لم يؤد إِلىٰ نهاية مفاجئة لقرن من الهيمنة الأمريكيَّة، على نحو ما تنبأت به وكالة الأَمن القومي تحت تأثير الهيستيريا التي طغت عليها يومذاك. غير أنّه أنار الدرب أمام جيل جديد من كتّاب الكريبتوجرافيا الذين حملتهم الجرأة على العمل خارجْ أسوار السرِّيَّة التي تقيمها الحكومة. وكان في مقدمة هؤلاء التلاميذ: هويتفيلد ديڤي.

ويقول ديڤي في وصف تجربته: «لقد قرأت الكتاب بعناية أكثر من أي

قارىء آخر. . . وكتاب كاهن «مفكّكو الشّيفرة» عندي مثل كتب الفيدا [كتب الحكمة المقدسة عند الهندوس]. وهناك قول [شائع عند البراهمة] «إذا أضاع الرجل بقرته، فعليه بالبحث عنها في أسفار الفيدا».

ولما انتهى ديڤي من قراءة كتاب كاهن «مفكّكو الشّيفرة»، وجد أنّه استوعب هذا العلم ولم يعد بحاجة إِلىٰ الاعتماد على الآخرين في معالجة القضايا الكبرى في الكريبتوجرافيا، فلقد غدا مستغرقاً فيها بكل وجدانه، وباتت تشغل أحلام يقظته، وها هي الآن هواه المقيم.

ما الذي جعل اهتماماً عارضاً عند ديڤي يغدو هوى مقيماً الآن؟ إن وراء كل كريبتوجرافي (واضع شيفرة) عظيم، على ما يبدو، علة مقيمة ملحاحة. ومع أن البحث الذي نهض به ديڤي كان في أساسه تحدياً فكرياً، فإن الرجل اعتبر مهمته تحدياً يرتبط بكرامته الشخصية. فلقد كان تحت لباسه العادي وشعره الأشقر الطويل، رجلاً ذا كبرياء وعزيمة وتصميم، وفي أعماقه دافع غير مألوف، يحمله على بلوغ ما يعتبره الحقيقة الأساسية في أي موضوع. وهذا كله أدّى به إِلىٰ الانشغال بحماية الأسرار، وعدم الكشف عنها، وخاصة الهامّة منها التي يحرص عليها أصحابها، ولا يبوحون بها، ويضحون دونها بما يملكون. ونجده يخبرنا اليوم: «إن ما حملني، في ظاهر الأمر، على الاهتمام بهذا الموضوع هو أهميته للحريَّة الشخصيَّة. بيد أنني كنت مسحوراً أيضاً باستقصاء هذا الموضوع الذي يتجنّب الناس الخوض فيه. وكأنما كان حل هذا اللغز سيأتي بمعنى أعم للعالم كله. ويقول في هذا: «أعتقد أنني بمعنى حقيقي جداً من الغنوصيين. ولطالما كنت أنشد طوال حياتي العثور على سرّ ما عظيم. . . أعتقد أنه في مكان ما من أعماق عقلي، ثمّة فكرة بأنني سأبرأ من الإثم إذا ما بلغت المعرفة الصحيحة.

وعندئذ تداخل بحث ديڤي عن الحقائق في الكريبتوجرافيا، بهوى من نوع آخر: غرامه بماري فيشر.

لم يقصد هويت ديفي أصلاً أن يقع في هوى مدربة حيوانات يهوديَّة من بروكلين ومتزوجة. فهي في الواقع تكاد لم تخطر بباله حتَّى ذلك اليوم الذي سمع فيه تقريعها على الهاتف لتجاهله لها. بيد أن غضبها أصاب منه وتراً حسّاساً، وربما كان ذلك بسبب من طول عهده بها. فهو يوم ودّعها، وكان يتهيأ للسفر إِلىٰ الطرف الأقصى من البلاد، وقال لها أنه سوف يعود للقائها بعد عام، كان جاداً في قوله. ولم يكن لديه من المال سوى 12 ألف دولار، هي مدخراته من عمله في شركة ميتري، وعزمه على «العيش على الكفاف»، على حد تعبيره، ليتمكّن من القيام بالسفر لتحصيل كل ما يستطيع تحصيله من العلم بموضوع الكريبتوجرافيا، بل ليكون له إسهام فيه. وبدا مشروعه أشبه بالمهمّة التي لا تحتمل شريكاً.

ولكن حين زار ماري وزوجها، في نيوجيرسي، في آب/ أغسطس 1973، وجد حياتها الزوجيَّة منهارة، والمرأة تجد عزاءها بارتياد تجمعات دينيَّة غريبة. ولم يكن ذلك من الأمور التي يمكن التحدّث عنها مع عالم رياضيَّات مثل ديفي، غير أنَّها حين أخذت تحدّثه عن ذلك، عجبت منه إذ سمعته يقول: «أتدرين يا ماري، إنني لطالما كنت أنجذب إِلىٰ المتصوفين». وهكذا انعقدت الصلة بينهما وأخذا يمضيان الوقت معاً. ولما كانت ماري فيشر لا تحسن قيادة السيارة، فقد اعتاد ديفي اصطحابها إِلىٰ حدائق الحيوانات ـ وخاصة للبحث عن الكوبرا الملكية ـ ثم في الرحلات الأبعد لمشاهدة الكنائس ذات الطراز المعماري المثير للاهتمام. وذات مرّة، بينما كان يقود السيارة في إحدى دروب ماساتشوسيتس، أوقف السيارة فجأة، بدافع من رغبة غلبت عليه، وقال لماري بهدوء شديد أنَّه يحبّها. وردّت عليه بأنَّها تحبّه بالمقابل. وكان هذا خاتمة الأمر. ومع أنَّه كان من المؤلم لفيشر بأن زواجها بلغ نهايته، فقد عمل ديفي على تسريع هذه النهاية بأن اقترح عليها مشاركته الإقامة في فلوريدا، ليشاهدا معاً إطلاق المركبة الفضائية سكايلاب. فانطلقا للتو إِلىٰ فلوريدا، وبلغا قاعدة

إطلاق المركبة في كيب كانافيرال في الثالثة صباحاً. وما هي إِلاً بضع ساعات حتَّى كانا يشاهدان معاً الصاروخ الضخم يلفظ النار وهو يقفز نحو الكون.

ومنذ تلك اللحظة غدت ماري فيشر رفيقة ديفي، ثم زوجته لاحقاً، فيما كان يقود سيارة قاطعاً الأميال بحثاً عن حلّ للغز الكريبتوجرافيا. وكان الزوجان يمضيان الوقت في الحديث أَو يغنيان، الأغاني الشائعة. ولم تكن وكالة الأَمن القومي لتدري في غضون ذلك، أن الرجل الذي سيقضِ مضاجعها، يقضي الساعات الطوال في سيارة داتسون 510، يغني مع رفيقته الجديدة لحن «كارولين العذبة». ومع أن فيشر لم تكن تلمّ إِلاً بالقليل عن التقنيات والرياضيَّات التي تشغل بال ديفي وتدفعه للعمل، إِلاً أَنها غدت مع ذلك شريكته في البحث. وباتت ملهمته في الكريبتوجرافيا.

وتستذكر ماري تلك الأيام قائلة: «كنت فزعة طوال الوقت لأنني هجرت كل ما كان مألوفاً. كان يتوقف بين الحين والآخر في إحدى المكتبات، أو لرؤية أحد الناس، وكانت تلك حقاً حياة حافلة بالأسرار، حياة عباءة وخنجر، أناس يتفادون التحدّث إليه، أناس يرفعون ياقة المعطف يغطون بها وجوههم، أناس يريدون معرفة كيف توصّل إِلىٰ اكتشاف أسمائهم، أناس يحملون أسراراً، ولا يريدون الكشف عنها. وكان هويت يحاول استخراج تلك الأسرار. كانت رحلة استكشاف متصلة لمثابرته على التحقق من أولئك الناس. كما كان يشركني أحياناً قائلاً: «أريد منك أن تقفي هنا وتصغي. لا أريد أن يراك أحد، إنما أرغب منك أن تصغي وحسب. وهكذا كنت أقوم بما يطلبه مني. لكنني بشكل أساسي لم يكن لدي أي فكرة عما ينوي القيام به».

وفي بعض الأحيان، كان ديفي يجهد نفسه لتفسير دوافعه لماري، وذات يوم قال لها: إن لعصر الكومبيوتر آثاراً رهيبة على أَسرار الإِنسان وخصوصيته. وقال محذِّراً، حينما تسود هذه الآلات ونستخدمها في اتِّصالاتنا اليومية، فإِنَّنا قد نفقد خصوصيتنا وحرّيتنا الشخصيَّة كما نعرفها اليوم إِلىٰ الأبد. ولقد أثارت

لهجته التنبّئية اضطراباً في نفس ماري، لكنها أرادت سماع المزيد.

أدركت ماري، في النهاية، أن الرسالة التي نهض بها ديڤي تمزج بين ما هو سياسي وما هو شخصي. فاكتشافه لحيلة يحمل بها وكالة الأَمن القومي على التخلي عن احتكار الكريبتوجرافيا، لم يرضِ نزعته إِلىٰ التمرّد على نحو ما كان مألوفاً لدى الشباب في الستينات فحسب، بل زاد كذلك مما بات يعرف به فيما بعد من نزعة أخلاقيَّة تحرّريَّة. وتخبرنا ماري عن هذا النزوع فتقول: «يريد هويت أن يكشف الأَسرار. إنه يسعى لمعرفة كل ما هو سر وسرّي. ولقد عجبت حين غدونا نعيش معاً، ولم أكن لأصدّق ما تراه عيناي. إذ وجدته يأتي بأمور عجيبة مثل البحث في أكياس القمامة. ذلك أنّه ما كان ليثق بأي شيء. وما يسلِّم به الناس باعتباره أمراً عادياً، هو عنده ضرب من التبسيط لا يقبل به، ولا بدّ في رأيه من أن يكون تحت السطح أكثر مما هو ظاهر. ثم تراه يبني بهذه الطريقة تعقيدات رهيبة.

كان أبرز التعقيدات، مهمته الدونكيشوتيَّة في ظاهرها، لاكتشاف بعض الأمور رغم أنف وكالة الأَمن القومي. وقد تساءل ذات يوم في سرّه، إن كان في ما يقوم به ضرب من المجازفة بنفسه، وكان قراره «تفادي لفت الأنظار خلال السنتين الأوليين». لكن ازدياد عوامل المجازفة، جعلت البحث أشد جاذبية وإغراء لديڤي.

كان الشيء الوحيد الذي محضه ديڤي ثقته خلال تلك الفترة هو سيارة الداتسون 510. فقد دأب على شراء العربات من هذا الطراز وإصلاحها وتعميرها، وإن كانت الشواهد تدل على ضعفها. وفسَّر ذلك بقوله: «كنت رجلاً عنيداً»، وأضاف: «كان معظم ما يصدر عني مبعثه العناد». أما ماري، فتعبر عن ذلك بشكل مختلف: «حين يقرّر هويت أمراً فإنه يعمد إِلىٰ استقصائه والبحث في مختلف جوانبه، ثم يركِّز على أفضل فكرة تناسبه، فإذا تم له ذلك ارتبط به ارتباط الزوج». كانت سيارة ديڤي الداتسون قد تعطَّلت ذات مرة في

نبراسكا، فاستأجر شاحنة لنقلها إِلىٰ الشاطىء الغربي. ثم عمد بعدئذ إِلىٰ شراء سيارة داتسون 510 أخرى، وكانت عربة سوداء اللون، خردة، مستهلكة، يشير عدَّادها إِلىٰ أنها قطعت 100 ألف ميل. ويقول في وصفها متذكِّراً إيَّاها بلهجة يخالجها الودّ: «كانت تجهيزاتها ممتازة من الداخل». وحملته هذه السيارة وماري في رحلته الثانية عبر القارة الأمريكية. وتداعت صحة السيارة في لامسيلا، بولاية نيوميكسيكو، ولم تنقطع عن إصدار صوت كأنَّه النذير، تشينك ـ تشينك. . . ، إِلاَّ أنَّها استطاعت أن تحمل هويت وماري، وتعود بهما إِلىٰ كاليفورنيا، ثم تهاوت وخمدت أنفاسها في موقف للسيارات في ريد وود سيتي بعد يومين من عودتهما من الرحلة. فاشترى ديڤي سيارة داتسون أخرى، وبدأ معها عملية استبدال للأجهزة بالغة التعقيد. وتخبرنا ماري فيشر: «كان لدينا في وقت من الأوقات خمس سيارات داتسون، يقوم هويت بإصلاحها جميعاً، فما كان ليثق بالميكانيكيين. والحق أنّه لم يكن بالرجل الذي ينزع بطبعه للثقة والتسليم».

وبعد، ترى ما الذي صادفه ديڤي في رحلاته عبر البلاد؟ لقد صادف الكثير ممن أعرضوا عنه وأنكروه. غير أن قلَّة من الناس قدَّموا له العون، ووفروا له بعض التلميحات إِلىٰ أساليب معاصرة في الكتابة بالشّيفرة، أَو لأعمال غير منشورة.

وكان من بين هؤلاء ملهمه ديڤيد كاهن، الذي دعاه لتناول البيتزا في داره، في لونغ آيلند، حين اتصل به يعرفه بنفسه. ومع أن كاهن دُهش لمنظر ديڤي ـ شعر طويل مسترسل، ولباس مهمل، إِلىٰ أبعد حد ـ إِلاَّ أن معرفته الواسعة وقعت عند صاحب كتاب «مفكِّكو الشّيفرة» موقعاً حسناً. فوافق يومذاك على تزويد ديڤي ببعض الوثائق المتصلة بالكريبتوجرافيا من أبحاثه.

كان من أهم البحوث التي وقع عليها ما يتصل بوليم فريدمان، الذي يُعتبر الأب الروحي للمجهود الحكومي في الكريبتوجرافيا. فقد جذبت الكريبتوجرافيا

اهتمام هذا الرجل الأمريكي الجنسيَّة والذي وُلد في روسيا في أواخر القرن التاسع عشر، أثناء بحثه في احتمال كون فرنسيس بيكون، المؤلّف الحقيقي لمسرحيات شكسبير، (دحض فريدمان وزوجه إليزابيث هذه الفكرة علمياً في كتابهما The Shakespearean Ciphers Examined دراسة الرموز الشكسبيرية). وقد شارك فريدمان أثناء الحرب العالمية الثانية في مجهود الحكومة الأمريكية لتفكيك الشيفرات، وأقام سلسلة من الدورات لتدريب محلّلي الشّيفرة. وغدت أعماله داخل تلك المجموعة المغلقة أعمالاً كلاسيكيَّة، وخاصة المتعلّقة باستخدام الإحصائيات لحل الشيفرات. وكان لعمل فريدمان في الحرب، الفضل في حلّ الشّيفرة اليابانية المعروفة باسم «القرمزية» Purple، وهو كان شخصية هامة في وكالة الأَمن القومي منذ بداياتها، وظل لفترة طويلة يعمل فيها مستشاراً حتى بعد تقاعده عام 1955. وبذلك فإن جميع أعماله الهامة كانت تُعتبر من الأسرار الخطيرة. وعندما قدم «كاهن» «الديڤي» بعض الأَعمال النادرة لفريدمان والتي باتت متاحة للاطلاع مؤخراً، تناولها وكأنما بين يديه نسخ أصلية من الدستور. وتجلى حرصه على تلك الأعمال بقيامه بتصوير كل صفحاتها بنفسه بآلة تصوير 35 ملم، بدلاً من تكليف أحد المستخدمين بتصويرها بآلة نسخ. وكان لذلك الحرص فائدة جلى، إذ أمكن بهذه الطريقة تجنّب لفت انتباه الوكالة إلىٰ تسرّب تلك البحوث من مستودعها الحصين وراء السور الثلاثي الذي يحمي مقرّها، فلما أدركت حقيقة ما حصل، حاولت أن تضفي السرّيّة على تلك الأوراق بأثر رجعي، فتفرض على من يحوز عليها إعادتها فوراً إلىٰ مصدرها، خشية ملاحقتها لهم بتهم جنائية.

وفي صيف 1974 بلغ مسامع ديڤي أن جيم ريدس، وكان طالباً يحضر لنيل شهادة الدكتوراه في علم الإحصاء من جامعة هارفارد، والتقاه قبل عام، يشرف على حلقة دراسية (سيمنار) في الكريبتوجرافيا. فعاد ديڤي إلىٰ كمبردج. وكان هناك، بعد، بيل مان، وهو صديق كان يعمل في الخطة الأمنية لوكالة

المشاريع والبحوث المتقدّمة (أربا ARPA). وفي إحدى المرَّات، حاول ديڤي أن يشرح لمان، معنى ما يسمى دالة (تابع) حسابية وحيدة الاتجاه One way function، وهي من مسائل الرياضيات الغريبة التي اعترضته، ولم ينقطع عن التفكير فيها منذ ذلك الوقت. وهذه الدالة (التابع) الوحيدة الاتجاه، هي أمر يمكن حسابه بسهولةٍ باتجاه واحد، إلاً أنه ليس من السهل عكسه ـ وقد وصفها أحد كتّاب الكريبتوجرافيا بقوله: إنك تعمل بها حين تكسر طبقاً. غير أنَّه ليس من اليسير جمع القطع الصغيرة المتناثرة لتعيد تشكيل الطبق من جديد.

وكان ديڤي يزداد يقيناً بأن الدالة الوحيدة الاتجاه يمكن أن تغدو منهجاً جديداً في الكريبتوجرافيا، لكنَّه لم يكن واثقاً من الطريقة التي يتحقَّق بها هذا المنهج. لكنه لم يستطع أن يشرح لمان بوضوح يمكِّنه من استيعاب الفكرة. مما أدّى إلىٰ إساءة مان فهم الفكرة على نحو مبدع، فخرج بانطباع مؤداه أن الدالة الوحيدة الاتجاه، ليست بالأمر الذي يمكن حسابه بيسر باتجاه واحد وحسب، بل يمكن حسابه معكوساً أيضاً، إذا توفرت لك المعلومات الصحيحة. فقال مان مستعيناً بمثل الطبق، إن الأمر أشبه ما يكون بأن يكون لدى المرء الذي كسر الطبق، طريقة سحرية لمنع كسره، مثل دوران شريط سينمائي معكوساً، ليعرض تلك القطع الصغيرة المتناثرة من الخزف، وهي تتجمع لتشكِّل طبق العشاء. وكان مان يتصور وهو يعرض فكرته لديڤي ما سوف يعرف ذات يوم بـ: الباب الخادع للدالة (التابع) الوحيدة الاتجاه Trap door one-way function، وبذلك فإن سوء الفهم ذاك كان أشبه ما يكون بالضارة النافعة.

وفي كمبردج أيضاً، تحدَّث ديڤي مع ريتشارد شرويبل في موضوع الكريبتوجرافيا. وكان شرويبل من قراصنة الكومبيوتر (المتسللين) في معهد ماساتشوسيتس (إم آي تي)، وله سمعة الساحر في الرياضيات، وباتت تراوده الآن فكرة التجارة الإلكترونية، بينما بدأ يخوض في القضايا ذاتها، التي خاض فيها ديڤي ومكارثي؛ مثل ماذا لو أن الشركة (أ) أرادت أن تخاطب الشركة

(ب)، إلكترونياً، في أمر شحنة من البضائع، ولم تكن بينهما علاقة من قبل؟ وكيف لهما أن يضمنا سرّيّة اتّصالاتهما؟

عجب شرويبل إذ وجد ديفي، قد أولى هذه القضايا الكثير من تفكيره. ولا ريب أنّه حمل التقدير لديفي الذي أنجز عملاً كبيراً، مع أنه غير معلن، في مختبر الذكاء الاصطناعي في إم آي تي، ودوره في وضع نظام المعالجة الرياضي ماكسيما. وكان يعلم أن ديفي هو واضع الطريقة المعقدة لمعالجة الأرقام الكبيرة في نسخة كومبيوتر ستانفورد اللغوي LISP (ليسب) ويقول شرويبل: «باعتقادي أن وضع طريقة لمعالجة الأعداد الكبيرة يضعك على عتبة عالم آخر. إنه أشبه باجتياز الامتحان؛ ومعنى هذا أنّك تعرف كيف تستخدم الكومبيوتر، وتعرف فعلاً إجراء الحساب».

وأثناء تناولهما الغداء في أحد الأيام، طرح ديفي فكرة إمكانية وجود طريقة للتغلّب على مشكلة التجارة الإلكترونية، واقترح عليه مسألة الدالة (التابع) الوحيد الاتجاه، دالة وحيدة الاتجاه قابلة للعكس، كتلك التي اقترحها بيل مان عن غير قصد. فهل يمكن أن تكون هذه جزءاً من الحل؟ واستمر الاثنان يبحثان في هذا الأمر لفترة، إلاّ أن شرويبل كان في شك من نجاعة هذا الحل، فقال محذّراً ديفي: «الواقع، أنّك ربما لا تجد هذه الدالآت (التوابع)، وعلى الأرجح أنّها غير موجودة».

إلاّ أن هذا الشك لم يردع ديفي، ولا فتّ من عضده، فتابع بحثه متشوقاً لمصادفة من يوفر له المزيد من المعلومات الموثوقة. فمضى وفيشر لمقابلة صديق في كمبردج كان قد حدّثه عن شخص يدعى ألان تريتر. وكان يُعتقد بأن لتريتر هذا نصيب من العمل في الكريبتوجرافيا، ويعمل الآن في شركة IBM آي بي إم. [الشركة العالمية للأجهزة التجارية International Business Machines Corporation هـ. م] فمضى ديفي في إثره في صيف عام 1974، فوجده في أكبر مركز للنشاطات الكريبتوجرافية خارج إطار الحكومة. والذي يحمل اسم مختبر

تي جي واطسون T. J. Watson، في شركة آي بي إم، بمقاطعة ويستشيستر، في ولاية نيويورك.

كان تريتر شخصية بارزة، حتَّى في حقل كهذا حافل بالعقول الفذَّة. كما كان ضخم الجثة، بديناً جداً بسبب مرض نادر أصابه مما جعل وزنه يصل إِلىٰ 400 رطل إنكليزي حسب قول أصحابه. وتروي الشائعة، أن جده كان رجلاً موسراً، لكنَّه لم يخلف له من المال، إِلاَّ ما يسمح له بمتابعة دراسته فقط. ولئن كان البعض يعتبرونه عبقرية رياضية، فإن هناك آخرين يرون أن شهرته لا تستند إِلىٰ أساس. ويذهب أحد زملائه القدامى في شركة آي بي إم في الشكوى إِلىٰ حد القول: «ما أن عُيِّن في الشركة حتَّى ندم القوم على قرارهم، لكن الشركة لا تعترف بخطئها». إِلاَّ أن تريتر كان، من الجهة الأخرى، متقدماً على زمانه، إذ أتقن التنصت عبر الهاتف باكراً. وقدر له أن يموت شاباً.

سرّ ديفي حين علم أن تريتر كان خبيراً عارفاً بالتحقق من الصديق والعدو (آي إف إف IFF) [Identification Friend or Foe]، وقد عجب ديفي أن يجد في كتاب كاهن إشارة إِلىٰ هذه المنظومات، وهي أجهزة اتصالات تمتحن بعضها البعض للتأكد من الهوية والتعارف. وتؤدي عملها، كما شرح تريتر لديفي، بطرح «تحد» كريبتوجرافي لا يمكن الرد عليه إِلاَّ باستخدام معلومات سرِّيَّة موضوعة على وجه التحديد لحل المشكلة. والوضع الذي يأخذ به نظام (آي إف إف ـ IFF) يصور طائرة مقاتلة تواجه في الجو طائرة أخرى أثناء فترة الاشتباكات. فإذا كانت الطائرة التي دخلت المجال معادية، وجب إسقاطها، إِلاَّ أنَّه من الواضح أن الحكمة تفرض تجنّب الاشتباك قبل التحقق، لئلا يكون الهدف صديقاً ويقع المحظور. فهذا النِّظام إذاً (آي إف إف) هو المعادل الإِلكتروني لسؤال الخفير جندياً يقترب من المعسكر عن «كلمة السر». إِلاَّ أنه أكثر اعتماداً على الإجراءات الإِلكترونية المعقَّدة منه على كلمات السر. وبما أن مثل هذه الاتِّصالات تجري عادة بالراديو، فالمفترض أن الأعداء يصغون إليها،

فإذا صدرت كلمة سر عامة إلىٰ قوات أحد الطرفين، فيمكن للعدو أن يكتشف سهولة، الكلمة السحرية التي تمكن طائرته من الظهور بمظهر الصديق.

ولقد صادف أن أحد زملاء تريتر في شركة آي بي إم، وهو عالم ألماني يدعى هورست فايشتل، قد نهض بعمل حاسم في هذا الحقل. (لسوء الحظ أن فايتشل، كان قد ذهب لقضاء عطلة نهاية الأسبوع في كيب كود، فلم يحظ ديفي بمقابلته يومذاك). وشرح تريتر لديفي كيف تغلبت أنظمة فايتشل للتحقق من الصديق والعدو على مشكلة التنصّت: حين تواجه الطائرة الأمريكية طائرة لم تتبيَّن هويتها بعد، ترسل إشارة راديو تحتوي على تحد يتم اختياره عشوائياً من بين عدد كبير من البدائل المحتملة. أما الطائرات الأمريكية الأخرى، فتكون مجهَّزة بالأجهزة اللازمة لتشفير تلك الإِشارة على الوجه الصحيح، ثم، تقوم بإرسال الإِشارة المشفَّرة إلىٰ من أرسل إشارة السؤال الذي يقوم بدوره بالتأكّد من هوية الطائرة بفك تشفير إشارة الرد. فإذا توافقت الإِشارتان، كانت الطائرة الأخرى أمريكية بالتأكيد. ولن يجدي الطائرات المعادية الإصغاء إلىٰ الرسالة وتكررها كردّ على السؤال، لأن الطائرات الأمريكية سوف تختار إِشارة مختلفة، تتحوّل إلىٰ إِشارة مشفَّرة مختلفة أخرى.

وجد ديفي المعلومات التي استقاها من فايتشل حافلة بالإِثارة. ذلك أن الشرح الذي قدَّمه يعني أن أَجهزة (آي إف إف) تعمل نوعاً ما بذات الطريقة المأمولة من الدالة الوحيدة الاتجاه. فاستمر في البحث آملاً بأن يصادف مثل تلك المعلومات المفيدة حينما يقابل ألان كونهايم، رئيس مجموعة الرياضيات في شركة (آي بي إم). لكنّه لم يحصل منه على شيء، وقد وصفه ديفي شاكياً: «كان شديد التكتم». كان كونهايم، الأستاذ حالياً في جامعة كاليفورنيا في سانتا باربرة، أحَد علماء الرياضيات الذين اتبعوا عدة دورات دراسية ترعاها وكالة الأَمن القومي، ووقَّع على الوثيقة المشؤومة، التي تلزم الدارسين بتسليم الوكالة أعمالهم المستقبلية في مجال الكريبتوجرافيا، وكان الأمر كما عبَّر عنه، فيما بعد، تعهداً أبدياً؟

حاول ديفي جاهداً مع كونهايم دون أن تلين له قناة؛ فما كان الرجل ليقبل بتقديم أي معلومات ذات شأن للغريب الجالس في مكتبه ذي الجدران الزجاجية المقوسة، في مبنى مركز واطسون للبحوث، إلاَّ أنَّه قدَّم له معلومة وحيدة هامة: «وما زال إلىٰ اليوم يتمنَّى لو أنه أمسك عنها». ولم تكن إشارة تتصل بالكريبتوجرافيا، بل إحالة إلىٰ شخص يطرح تساؤلات كالتي كان ديفي يطرحها؛ وكان هذا قد عمل حيناً في مختبر الشركة، ويعمل الآن أستاذاً مساعداً في جامعة ستانفورد، واسمه مارتين هيلمان. واقترح كونهايم على ديفي أنه ربما يتمكَّن رجلان من معالجة معضلة بشكل أفضل مما يستطيع رجل واحد القيام به.

بعد أن وصل ديفي وماري إلىٰ الساحل الغربي، في رحلتهما الثانية، بسيارة من تلك السيارات الداتسون 510 العتيقة، لينزلا في بيت جون مكارثي، كان أول ما قام به ديفي أنه اتصل هاتفياً بأستاذ الهندسة الكهربائية الشاب هيلمان. ويقول مارثي هيلمان الآن مستذكراً: «لقد رتبت موعداً لمقابلة تستغرق نصف ساعة في مكتبي في ستانفورد، وكنت أعتقد أن المقابلة لن تكون مثمرة. إلاَّ إنني قبلت مع ذلك باللقاء، بصرف النظر عن النتيجة». وكانت ثمرة هذا اللقاء قيام ثنائي قيض له أن يكون في عالم الكريبتوجرافيا، من الشهرة ما لغيره من الثنائيات الشهيرة أمثال: وودورد ـ بيرنشتاين. لينون ـ مكارتني. واطسون ـ كريك.

ديفي ـ هيلمان Diffie-Hellman

بالرغم من أن مارثي هيلمان عاش في كاليفورنيا، إلاَّ أنه نشأ وترعرع وسط مدينة نيويورك، وشبَّ فيها فتى مقاتلاً. وكان يبدو بشعره الأسود ولحيته ونظرته المتوترة المحدقة، أشبه بنسخة سامية Semitic من مارتين سكورسيسي. ولد هيلمان سنة 1945، يهودياً في حي كاثوليكي قاس، وتعلّم أن يتمثل وجهة

نظر الغريب عن الوسط. كذلك اتخذ العلم ملاذاً له. وكان والده وعمه مدرّسان للفيزياء في المدارس العامة. أما الفتى هيلمان، فلطالما افتتن بالمكتشفين والاكتشافات الجديدة، سواء كان ذلك ماجلان يمخر عباب البحار إلىٰ العالم الجديد، أم آينشتاين وهو يعيد رسم طريقنا لفهم الكون. وتم قبوله في عداد طلاّب ثانوية برونكس للعلوم؛ وكانت هوايته التحادث بالراديو. وفي هذا يقول: «لعل ذلك ما اجتذبني إلىٰ هندسة الكهرباء، وهو مجال واسع جداً؛ تستطيع الانتقال فيه من الفيزياء النظرية، إلىٰ فيزياء المواد الصلبة والرياضيات». ثم نال الدكتوراه من جامعة ستانفورد، عام 1969، وكانت وظيفته الأولى في قسم الأبحاث، في شركة آي بي إم، في يوركتاون هايتس، في نيويورك.

ولم يكن قد مضى على هيلمان فترة بالعمل في الشركة حين قدم بحثاً في ندوة علمية حول نظرية المعلومات، أقيمت في فندق ومنتجع نيڤيل، مقر شركة كاتسكيلز بورتشت بليت Catskills Broscht Belt، وكان المتحدّث في مأدبة العشاء التي أقيمت للمشاركين: ديڤي كاهن، ولئن كان هيلمان يرى دوماً في الكريبتوجرافيا غواية وإغراء، فإن حديث كاهن هناك، حمله على النظر إلىٰ الموضوع كدراسة علميَّة جادّة، ثم ازدادت هذه الخواطر قوّة حين وجد أن ربّ عمله الجديد ذو شأن في هذا الحقل. وخطر بباله حينذاك أن في الأمر مصلحة تجارية بلا ريب. ومع أن هيلمان لم يعمل مع هورست فايشتل بشكل مباشر، إلاّ أن وجود الاختصاصي بالكريبتوجرافيا، والألماني المولد قريباً منه في المبنى، جعله على احتكاك به، فكان يصادف جلوسهما معاً لتناول الغداء أحياناً، وعندئذ يقوم الكهل بعرض بعض منظومات الشّيفرة الكلاسيكيَّة وشيء من أساليب تفكيكها.

في عام 1970 ترك هيلمان عمله في شركة آي بي إم، ليشغل منصب الأستاذ المساعد في معهد ماساتشوسيتس للتكنولوجيا (إم آي تي). وكان بيتر إلياس الذي سبق له العمل مع كلود شانون، على وشك أن يترك رئاسة كلية

الهندسة الكهربائيَّة. ولقد دفع حديث إلياس، الأكاديمي الشاب، ليزداد تعمّقاً في مجال الكتابة بالشّيفرة، وبدأ يفكِّر لأول مرة بأن يجعل منه موضوع أبحاثه. ويفسِّر ذلك الهوى الآن بقوله: «إن مرد ذلك جزئياً ما يتيحه هذا المجال من الاضطلاع بدور الساحر، وانتزاع إعجاب الناس بخدع سحريَّة، بالإِضافة إِلىٰ أنَّه ينطوي على إمكانية ممارسة تأثير حقيقي، والارتقاء في حياتي المهنية عن هذا الطريق».

قاوم هيلمان الإغراء بالاقتداء بالغالبية العظمى من العلماء والأكاديميين في حقله: العمل ضمن القيود الصارمة التي تضعها وكالة الأَمن القومي، وقال: «لقد استهدفني القوم في الوكالة منذ البداية، وحين سمعوا باهتمامي بالكريبتوجرافيا، شرعوا يضيقون علي ويثبّطون من عزيمتي». فصارحهم باهتمامه بالاستماع ومعرفة ما لديهم، شرط أن تكون له حرية نشر اكتشافاته. فحذَّره المسؤولون من أنَّه يبدِّد وقته دون طائل، وأنه بحرمانه نفسه من الاطلاع على البحوث التي أُنجزت في «القلعة»، لن يقيض له أن يأتي بشيء يستحق الذكر. لكن هيلمان، وكان يضطرم غضباً ويتّقد حماساً في تلك الأيام، ردّ عليهم بما معناه: اذهبوا إِلىٰ الحجيم، فسأتابع عملي مهما تكن العقبات! وما حمله على هذا السلوك، اعتقاده بأن جهده لن يذهب هباء، وإن انتهى بإعادة اكتشاف ما هو مدون في الكتابات التي يحظر الإطلاع عليها، إذ يمكن الاستفادة من اكتشافاته في الأغراض التجاريَّة. وكان «في ذلك العمل مشقّة، لكنَّه عمل مثير إذ لم يكن يعمل في هذا المجال أحد آخر».

يدخل ديفي

يصف هيلمان اللقاء بقوله: «كان لقاؤنا لقاء عقول متوافقة». وجاء هذا اللقاء في الوقت المناسب: ذلك أن هيلمان كان قد نشر قبل وقت قليل أوّل بحث له في حقل الكريبتوجرافيا ـ وهو تلخيص لعمل شانون ـ وتوقف عن الكتابة بانتظار عمل آخر يتبعه، وبات يتوق إِلىٰ أذن صاغية؛ ويقول في ذلك:

«كنت أعمل في فراغ، وأتساءل في خلدي إن كان في الأمر أي جدوى؟ وأصبحت قلقاً حول ما إذا كان البحث سوف يقودنا في نهاية المطاف إِلىٰ نتيجة».

حين ظهر ديفي مرتدياً ما وصفه هيلمان «لباس الذكاء الاصطناعي» ـ بنطال أسود، وجوارب بيضاء، وقميص أبيض، وحذاء تنيس ـ بدا ملفتاً للنظر. بيد أن الرجل كان متمكّناً ضليعاً في مجاله. ومعرفته تعادل مجلدات من الكتب. وإن شخصاً مثل هيلمان ناطح متاري الكيبتو السرِّيَّة، يستطيع تقدير كم أحسن ديفي، استغلال الشهور والسنوات التي قضاها في الترحال والتحدّث إِلىٰ كل من يستطيع مقابلته، والبحث في المكتبات عن كتب منسية مثل كتاب لويجي سالو في الكريبتوجرافيا والصادر عام 1938، والانكباب على دراسة نصوص غامضة مثل بحوث فريدمان التي حاولت وكالة الأَمن القومي تصنيفها، فيما بعد، بين الأَعمال المحظورة بأثر رجعي. ولهذا يقول هيلمان: «لقد استخرج كل ما فاتني أن أحظى به، أَو كانت قواي أوهن من أن ألتفت لاستخراجه». وأخيراً، ها هو ذا يصادف من يستطيع أن يتجاذب وإيَّاه الحديث في المسائل التي تشغله، ذهاباً وإياباً؛ فكان الأمر أشبه بلعبة أنيقة تجري بين لاعبي كرة محترفين.

استمر اللقاء بينهما الذي حدد له نصف ساعة، مدة ساعتين. ذلك أن اللقاء طاب لهيلمان ولم يكن يريد له أن ينتهي، كذلك يبدو أن ديفي أيضاً كان يريد للحديث أن يستمر أطول ما يمكن. كان هيلمان قد وعد زوجته بالعودة عند العصر ليقوم برعاية طفليهما في غيابها، ولما وجد الحديث بينهما متّصلاً، سأل ديفي إن كان يود اصطحابه إِلىٰ المنزل. فأجابه أن ليس في الأمر مشكلة. فما كان عليه سوى الاتصال بماري التي استجابت للدعوة، وجاءت لتناول العشاء مع هويت وآل هيلمان، وقد استمر الحوار بين الرجلين دونما انقطاع حتَّى الساعة الحادية عشرة ليلاً.

واتفق الاثنان، على متابعة الحديث. ويقول هيلمان عن ذلك: كان حديثاً فضفاضاً لا حدود له. كان لديه بعض الأفكار العظيمة، كما كان لدي، وكانت بعض أفكارنا تتداخل. وقد طاب لنا متابعة الحديث. ولم نكن نرمي الوصول إلىٰ هدف في هذا الموضوع أَو ذاك ـ كنا نريد أن نسير قدماً في هذا الدرب الذي قطعه كل منا دون أن نلقى في نهايته من يكرِّر علينا ما دأب الآخرون على قوله من أننا نبدِّد وقتنا هباء.

كان ديفي وهيلمان، كلاهما، يؤمنان إيماناً راسخاً بأن ظهور الاتصالات الرقميَّة، يجعل الكريبتوجرافيا التجاريَّة ضرورة لا مناص منها. ذلك أن شبكات الكومبيوتر والهاتف الضخمة قد يسَّرت على المتنصّتين أمر حياتهم إلىٰ حدّ يفوق التصوّر ـ وسيكون بالإِمكان تتمة التجسّس كلياً. كان راصدو الإذاعات مضطرّين، على الأقل، لرصد نقاط عديدة على الموجة الإذاعية؛ أما في حالة وجود شبكة، فإن الأمر يبدو، وكأن الناس جميعاً يبثّون إذاعاتهم على القناة ذاتها. فبوسع وكالة تجسّس، مثل وكالة الأَمن القومي ـ ولسوف تستطيع ـ أن تشغل الهوفر (المكنسة) فتشفط جيجا بايتات giga bytes من البيانات. ويخبرنا هيلمان: «إن تسعاً وتسعين بالمئة مما تسحبه يطرح في الجو هواء حاراً، ولكنكّك بتمشيط البيانات بحثاً عن كلمات مفتاحية، وعبارات وأسماء وعناوين أساسيَّة، تجد واحداً بالمئة من المعلومات قد سقط في جعبتك مادة ملموسة هامَّة».

إن الترياق لهذه الحال يعني، في جوهره، ثورة كريبتوجرافية، مما يتيح للناس العاديين تشفير الرسائل التي يبعثون بها عبر الشبكة. لكن المشكلة الكبرى، كما عرضها ديفي لمكارثي وشرويبل، إنما تكمن في تنظيم الكتابة بالشّيفرة ليفيد منها أكبر عدد من مستخدمي الشبكة وتيسير كتابتها لهم. ولا بدّ عندئذ من إيجاد ما يحل محل الطريقة القديمة، الشكل الكلاسيكي من مفتاح الشّيفرة المتماثل (حيث يقوم المفتاح ذاته الذي استخدم لتشفير النص، بتفكيك

النص المشفّر أيضاً)، أَو تعديل تلك الطريقة على الأقل، لأَنّها غير ملائمة إطلاقاً لمعالجة العدد الهائل من المحادثات، والتعاملات الرقميَّة التي تجري بين الناس. فالمشكلة تكمن في أنَّه يتحتّم على طرفي الحديث كليهما، أن يتفقا سلفاً على المفتاح الذي سوف يستخدمانه في محادثاتهما الخاصَّة، ثم يستخدمانه بطريقة ما، تحول دون كشفه للمتنصتين أَو المتطفلين. وهذا عمل بسيط نسبياً لمنظمة عسكرية، إِلاَّ أَنَّه كابوس مقيم في سوق يضج بالحركة. فما العمل - هل ترسل ملايين المراسلين إِلىٰ الشوارع، ليسلموا باليد مفتاحاً جديداً لشخص معين، كلما أراد أن يجري مكالمة هاتفيَّة أَو يسجِّل طلباً لبضاعة؟ وبدا عندئذ أن الطريقة الوحيدة المتاحة لمعالجة هذه الحالة، إنما تكون بتشييد بنية أساسيَّة لمراكز توزيع المفاتيح تكفل طرح مفتاح جديد كلما أراد شخصان إجراء مكالمة خاصة بينهما. لكن هيلمان كان يشارك ديفي شكوكه العميقة في جدوى مثل هذا النظام المركزي.

يقول هيلمان: «كنت أعلم أنه [ديفي] سوف يقيم بيننا قرابة الشهرين، ولكن كان ثمة شعور يخامرني بأنَّه قد يغادرنا في أي لحظة، وكنت حريصاً حقاً على بقائه هنا». وهذا ما دفعه لأن يتصل بالمسؤول عن المنح في المؤسَّسة القومية للعلوم NSF National Science Foundation ويسحب منه مزيداً من المال لإنفاقه على العمل في مجال الكريبتوجرافيا. وهذا كان كافياً لتوظيف هويت ديفي بصفة باحث بدوام جزئي. ويشرح هيلمان الوضع بقوله: «كانت المنحة ربما تكفي لعمل يتراوح ما بين عشر ساعات إِلىٰ عشرين ساعة في الأسبوع، أَو ما بين ربع إِلىٰ نصف ما يكسبه العامل عادة». كما أشار هيلمان على ديفي أن يستغل المناسبة لمتابعة الدراسة لنيل الدكتوراه.

لكن هذا الجانب من الترتيب، لم يقيض له أن ينجح. ويفسّر هيلمان ذلك في تحليله لشخصية ديفي بقوله: «كان ذا روح طليقة حقاً. فإذا كان معنياً بأمر يشغله دون أن يفسره له أحد، كرّس له الساعات الطوال يومياً، واكتفى

بالقليل من النوم، ولكن [ليس ذلك] شأنه حين يطلب منه القيام بواجبات دراسية». ولقد تخلّى ديفي عن متابعة برنامج الدراسة، حين لاحظ الإداريُّون أنّه تخلّف عن فحص مادة الفيزياء: «لم يطب لي القيام به وانشغلت عنه» ذلك كان تعليله للأمر. وبالرغم من محاولته تدبّر الأمر باللباقة والكياسة، فإنَّه تخلّى عن هذه اللباقات، حين رفض البيروقراطيون في ستانفورد تسجيل اسمه للإعداد لنيل الدكتوراه دون إثبات على أنّه درس الفيزياء، فقال لهم اذهبوا إِلىٰ الحجيم.

ويقول مارتي هيلمان: «كنت أرى في [افتقار] هويت ديفي [للدكتوراه] عائقاً، ولكن لعله بلغ النضج في سن مبكرة مما جعله يرد [على من يتطلبون الشهادات العليا] اللعنة علي إن اتبعت قوانينكم الغبية. ولعل بعضهم كان غبياً فعلاً».

وفي المحصلة فإن ديفي، استطاع تحقيق قفزاته حينما تساءل حول القواعد المتفق عليها في الكريبتوجرافيا ووجد أن بعضها «تافهاً». ومن الأمثلة على هذا: الاعتقاد بواجب التعامل مع متطلبات أمن منظومات الكتابة بالشّيفرة بأقصى درجات السرِّيَّة. إن هذا قد يصدق في حالة المنظمات العسكرية، أما في عصر الكومبيوتر، فإنَّه ضرب من الهراء. ذلك أن هناك عدداً غير محدود من الناس الذين يستخدمون الكومبيوتر ويحتاجون إِلىٰ نظام يحمي أسرارهم وخصوصيتهم؛ وغني عن القول، أنّه لا مناص من تعميم مثل هذا النظام بحيث لا يصعب على من يسعى إِلىٰ فكّ الرموز، بلوغه، والفرص لديه كثيرة للتدرب على تذليل صعوباتها. والأحرى أن تكون السرِّيَّة في موقع آخر في هذا النظام. ولعله من المفيد التوسّل بتلك التوابع الوحيدة الاتجاه، التي طالما شغلت ديفي.

توطدت العلاقة بين هيلمان وديفي في الشهور التالية، ورسخت بينهما روابط الزمالة والصداقة، حتّى أصبح هويت وماري يكثران التردّد على هيلمان وزوجته. وكانت دوروثي زوجة مارتي هيلمان، تهوى الكلاب الأصيلة ـ وغني عن القول أن هذا الموضوع كان يستهوي ماري أيضاً ـ ثم كان أن أثارت ماري

في إحدى بنات آل هيلمان الاهتمام بالعزف على الهارب. وجرت العادة على أن ينزوي هويت ومارتي، فيما الزوجتان والبنات منشغلات بشؤونهن، والرجلان منهمكان في الحديث في أمور الكريبتوجرافيا.

توصّل هويت وماري إلىٰ تفاهم بأن حياة الترحال قد انتهت. وكانا يقيمان يومذاك في دار جون مكارثي في بالو آلتو لرعاية ابنته المراهقة سارة، أثناء غياب ذلك العالم الرائد في الذكاء الاصطناعي، الذي يمضي سنه باحثاً في اليابان؛ وقد أخذا بالبحث في غضون ذلك عن بيت خاص بهما في بيركلي. ووجدت ماري وظيفة في شركة بريتش بتروليوم في سان فرنسيسكو. فكان هويت ينفرد بنفسه بالبيت طوال اليوم ويقوم بأعمال التنظيف والطهي. وكان يعمل بشكل أساسي مع مارتي عاقداً الأمل بأن تؤتي السنوات التي أمضاها في الدراسة والبحث ثمارها، ويقدم مساهمة مهما كانت ضئيلة في حقل الكريبتوجرافيا المحاط بالتكتم إلىٰ حد يثير الجنون.

إن سنوات الهوى لم تنل من هيامه بالموضوع. لا، ولم يشغله عنه الودّ العميق الذي يكنّه لماري فيشر، غرامه الآخر. بل على العكس، فقد زادت العلاقة بينهما من شدّة توقه للخصوصية، والبحث عن التكنولوجيا التي توفرها. كانت ملحمة بحثه قد بدأت من افتقاده الثقة بأنظمة الكومبيوتر والقائمين عليها. وها هو ذا الآن يجعل محوره الحفاظ على علاقة شخصية غالية أيضاً. وتفسّر ماري فيشر هذا التطور لاحقاً: «حين شعر بأنّه وقع أخيراً على شخص جدير بالثقة، غدا السؤال عنده: كيف تتعامل مع شخص جدير بالثقة في عالم حافل بمن لا يستحقها؟».

المعيار

في 17 آذار/ مارس 1975، صدرت وثيقة حكومية جافة أحدثت موجة من الصدمات كادت أن تنزع الغطاء عن عملية الشّيفرة المتواضعة التي كان يقوم عليها مارتين هيلمان في جامعة ستانفورد. وكانت [الوثيقة] تتضمن الإعلان عن إنشاء مكتب السجل الاتحادي Federal Register، في المكتب القومي للمعايير NBS National Bureau of Standards إن بي إس. ويدل ظاهر الأمر، على أنه واحد من مشاريع لا حصر لها في جدول أعمال تلك الوكالة، والتي إن اعتمدت أصبحت القناة الرسمية في التعامل مع الحكومة، بالإِضافة إِلىٰ أنَّها ستغدو المقصد السهل، للصناعة الخاصّة، وكل من هبّ ودبّ. وتضمن الإعلان أمراً قلَّما يرد في النشرات العلنية، تقديم خوارزمية تشفير جديدة كل الجدّة. وفوق هذا منيعة. وستعرف باسم معيار تشفير البيانات Data Encrytion Standard أَو اختصاراً DES ديز (كما يلفظ).

كان فريق العمل في ستانفورد قد بلغه أَن هذه الخطوة الجديدة آتية بلا ريب ـ إذ سبق أن وجّه المكتب القومي للمعايير (إن بي إس) دعوات لتقديم مثل هذا المعيار ـ كما كان هيلمان يعلم أن زملاءه القدامى الموثوقين في آي بي إم IBM، يعملون على وضع نظام موافق لمعيار الحكومة. ولذلك رحّب الفريق

بالإعلان في بداية الأمر. ويستذكر هيلمان تلك اللحظة: «كان ذلك نبأ عظيماً. فقد أسعدنا أن نجد معياراً يعتمد في هذا الموضوع، وهلَّلنا له باعتباره أمراً رائعاً».

ثم أخذ القوم في دراسة منظومة معيار تشفير البيانات فعلاً ـ وعلموا أن لوكالة الأَمن القومي على ما يبدو يداً في نشوئه. فتحول حماسهم بعدئذ إِلىٰ فزع ورعب. وبدا جلياً منذ اللحظة الأولى أن الحل في الـ ديز DES، يكمن في حجم مفتاح التشفير، وكان قياساً مترياً يحدّد مباشرة مقدار قوة النِّظام الكريبتوجرافي. وكان يبلغ 56 بت Bit طولاً، وهو رقم مزدوج لـ 56 موقع. وبوسعك أن تتخيّل هذا في صورة سلك فيه 56 قاطع كهربائي لتشغيل أَو إغلاق كل واحد منها. ومع أن (2^{56}) هو عدد ضخم في معظم الأحوال، إذ يعني وجود (2^{56}) مفتاحاً محتملاً أَو حوالى 70 كدريليون Quadrillion [رقم مؤلَّف من 1 وإِلىٰ يمينه 15 صفراً. هـ. م] إِلاَّ أن هيلمان وديفي ذهبا إِلىٰ أن هذا العدد، يعتبر صغيراً جداً بالنسبة لتشفير عالي المستوى. وكان اعتقادهما الثابت أن الكومبيوترات المتطورة، سوف تجهد نفسها، حتَّى تجد الحلول لمثل هذه الرسائل المشفَّرة، عن طريق «البحث الموسع»: أي تجربة بلايين المفاتيح المركبة بسرعة البرق، حتَّى تكتشف المفتاح الصحيح، الذي يجعل الرسالة تنتقل فجأة إِلىٰ عالم النصوص الواضحة. وهذا مثال كلاسيكي على «الهجوم بالقوة الغاشمة». ويقول هيلمان: «إن مفتاحاً كبيراً لا يكفل الأمن، لكن مفتاحاً صغيراً كفيل بتعريض الأمن للخطر».

ولقد كتب ديفي هذا المعنى في تحليل مبدئي للمعيار جدير بالاحترام، وقدَّمه في أيار/ مايو 1975، في نطاق تعليق عام، دعت إليه وكالة الأَمن القومي: «إن حجم المفتاح يكاد ألاَّ يكون مناسباً، إِلاَّ قليلاً، في أحسن الأحوال. وحتَّى في هذه الأيام، فإن العتاد (هاردوير) القادر على التغلّب على النظام بالبحث الموسع، قد يثقل على ميزانية أي منظمة استخبارات ضخمة،

لكنَّه على الأغلب لن يتجاوزها». وذهب إِلىٰ القول، أن مؤسَّسة تتمتع بحرية الإنفاق قادرة على تصنيع آلة، مصمَّمة حسب المواصفات المطلوبة، تستطيع فكّ أَسرار مثل هذا المفتاح في غضون يوم واحد. وكتب يقول: «رغم أن تحليل الشّيفرة عن طريق البحث الموسع ليس رخيصاً، لكنَّه مع ذلك ليس مستحيلاً. بل إن أقل تحسّن يطرأ على أسلوب تحليل الشّيفرة، كفيل بأن يغير من التناسب بين الكلفة والأداء. إننا نقترح مضاعفة حجم مجال المفتاح حرصاً على منعة النظام».

اعتقد ثنائي ستانفورد عن سذاجة، أن حكومة الولايات المتّحدة ربما ستأخذ بهذه النصيحة: حسن، الواقع أنكما مصيبان فيما ذهبتما إليه! فلنضاعف حجم ذلك المفتاح السخيف! ولكن ما حدث أن استجابة الحكومة جاءت على قدر من المراوغة، مما حمل هيلمان على الارتياب بحقيقة دوافع المكتب القومي للمعايير. ثم أخذ هيلمان في الشهور اللاحقة، يشكّك علناً في تلك الدوافع، متسائلاً إذا لم تكن خوارزمية معيار تشفير البيانات، خدعة جريئة من جانب الحكومة، لا لتضليل المواطنين فحسب، بل الأعداء الخارجيين كذلك، وإيهامهم بأنَّها تقوم بحماية المعلومات من التسرّب، في حين أن وكالة الأَمن القومي تستطيع الوصول إِلىٰ هذه المعلومات التي يفترض بأنَّها في حرز أمين. وتساءل هيلمان؛ وهو في أقصى درجات جنون الشك، إن لم يكن لمعيار التشفير «باب خلفي» زرعه فيه الكريبتوجرافيين الدهاة في فورت ميد. ومع أنَّه ليس هناك دليل مباشر على صحَّة هذا التساؤل، لكن، كان ثمة سبب يبرِّر الشكّ. كان هيلمان يريد أن يعرف لماذا تُعامل مبادئ تصميم الخوارزمية وأعمالها الداخليَّة كأسرار حكومية، إذا كانت الأمور مطروحة علانية، وتجري أمام الملأ؟ ثم، إذا لم يكن لدى الحكومة ما تخفيه، فلماذا تقوم بإخفاء بعض الأمور؟

كان هيلمان وديفي أول من طرح التساؤل حول الأصول الملتبسة لمعيار

تشفير البيانات. إذ استمر الجدل حول هذا المعيار حتّى حينما أصبح شبيهاً بمعيار الذهب في تحديد منعه الكريبتوجرافيا التجارية، وغدا موضوعاً لشكّ دائم بين الغرباء عن عالم الشّيفرة والحريات المدنية. ولم يتضح أن نشوء وإجازة معيار التشفير كان بمعنى معين قصة ملهمة إلاّ بمرور الزمن، قصة ذات عناصر مشتركة مع البحث الذي كان يقوم به ديفي وهيلمان.

بدأت القصة مع أحد أشد الباحثين غموضاً في شركة آي بي إم IBM هورست فايشتل. كان هذا الاختصاصي بكتابة الشّيفرة الألماني المولد والذي عمل في وضع قواعد برنامج التحقق من الصديق والعدو هو الذي اطلع عليه هويت ديفي عن طريق ألان تريتر. وكان فايشتل يعمل في قسم البحوث لدى شركة آي بي إم في يوركتاون هايتس منذ أواخر الستينات، وعمله من الأعمال القليلة في القطاع الخاص التي تُعنى بالبحث في الكريبتوجرافيا.

والحق أن بعض زملائه راودهم الشكّ بأن فايشتل كان يعمل في خدمة وكالة الأَمن القومي، ولعلَّه ما زال مرتبطاً بها بشكل من الأشكال، حتّى أثناء عمله في شركة آي بي إم. ذلك أن سيرته الذاتية لا تنبئ، بالكثير. وما يُعرف عنه، أنَّه وُلد عام 1914 وغادر ألمانيا شاباً. وكانت عمته قد تزوجت من يهودي سويسري يقيم في زيوريخ، وانضم إليهما فايشتل بحجة العناية بالعمّة في مرضها، قبيل بدء الرايخ الثالث بالتجنيد، ولولا ذلك لما أمكنه الهرب من ألمانيا. وبعد دراسته في سويسرا رحل إلىٰ الولايات المتّحدة عام 1934. وقبيل أن يكتسب الجنسية الأمريكية، دخلت الولايات المتّحدة الحرب العالمية الثانية، فوضع قيد ما وصفه ذات يوم بـ «الإقامة الجبريَّة»، واقتصرت تحركاته على منطقة بوسطن حيث كان يقيم. لكن أحواله تغيّرت فجأة، ففي كانون الثاني/ يناير 1944، مُنِح الجنسية الأمريكية بالإِضافة إلىٰ حصوله على إجازة أمنية ووظيفة في موقع بالغ الحساسيَّة، مركز كمبردج للبحوث التابع لسلاح الجو.

أمًا طبيعة عمله في ذلك الموقع فليست واضحة، ولقد كان شغوفاً بالرموز منذ فتوته، لكنَّه أسر لديڤي في أوائل التسعينات، بأنَّه، وإن كان راغباً بالعمل في مجال الشّيفرة، فقد أعلم بأن هذا ليس بالعمل المناسب في أثناء الحرب لمهندس ألماني المولد. ولكنَّه من جهة أخرى، قال في مقابلة مع ديڤيد كاهن أنَّه عمل حينذاك على أنظمة التحقّق من الصديق أَو العدو. لكن ليس في الكريبتوجرافيا حصراً.

ثمة تناقضات في روايات فايشتل الأخرى عن نشاطاته. فقد روى لديڤي أنَّه كان عليه قبل منحه الجنسية الأمريكية أن يُعلم السلطات كلما غادر بوسطن لزيارة أمّه في نيويورك. لكنَّه قال لأحد العاملين معه ذات مرة أن والدته، لم تهاجر إِلىٰ الولايات المتّحدة حتّى بداية الحرب الباردة. كذلك يروى عنه قوله أن الولايات المتّحدة هي التي قامت بتهريبها من برلين الشرقية، تحسباً للعواقب في حال اكتشف السوفييت، أن ابنها يعمل في مجال الشّيفرة وأرادوا الضغط عليها.

إِلاَّ أنَّه من المؤكد أن فايشتل، شرع يختص في أنظمة التحقق من الصديق أَو العدو (آي إف إف) بعد الحرب. فقد رأس حينذاك مجموعة من الباحثين في الكريبتوجرافيا في مركز كمبردج للبحوث، وكان من مهامه اجتياز نظام تعرّف متطور يعتمد على اختراع جديد مذهل هو: الترانزيستور. وقد أمكن بهذه الأعجوبة الدقيقة تصنيع جهاز آي إف إف صغير إِلىٰ حد يمكن وضعه في مقدمة طائرة مقاتلة. وهناك مشروع هام آخر كان شاغل فايشتل لفترة طويلة، هو تصميم نظام تشفير منيع يعتمد على كتلة من الشّيفرات. (يقوم هذا النسق على تشفير الرسائل بتقديمها في مجموعات أَو كتل، مقابل الشّيفرات المتدفقة التي يتم تشفير نصها أثناء جريانه أَو تدفقه).

هل أُعجبت وكالة الأَمن القومي بعمل فايشتل، أم أنَّها رأت فيه خطراً فحاولت خنقه؟ حسب رواية فايشتل لديڤي، كان العاملون في القلعة، فورت

ميد، قد رصدوا عمله في سلاح الجو، وتوسّلوا بسلطة الوكالة لتوجيه عمله الوجهة التي يريدونها، لكن الوكالة اعتبرت مشروعه مصدر تهديد أيضاً، واستطاعت في النهاية القضاء على مشروع الشّيفرة كلّه في مخبر كمبردج. ولما انتقل فايشتل في منتصف الستينات إلىٰ العمل في شركة ميتري (شركة التعهدات العسكرية التي قامت فيما بعد بتوظيف هويت ديفي)، حاول دونما طائل تنظيم مجموعة هناك لاستئناف عمله في مجال الشّيفرة. وقد عزا فشله للضغط الكبير الذي مارسته وكالة الأَمن القومي لإحباط مشروعه.

ولذلك أخذ بنصيحة صديقه. آ. أدريان ألبيرت، ومضى ليعمل في شركة آي بي إم، التي بدت أكثر انفتاحاً للأخذ بمثل هذه الاهتمامات. (كان ألبيرت رياضياً، ويرأس الجمعية الأمريكية للرياضيات، وله باع طويل في كريبتوجرافيا في الحكومة). وكانت شركة آي بي إم غنية إلىٰ حدّ يثير الدهشة، ومنافسوها قلائل، وكان قسم البحوث فيها مرتعاً فكرياً يلقى فيه علماء أفذاذ، التشجيع للبحث في كل ما يثير اهتمامهم. ويقول آلان كونهايم، الذي غدا رئيس فايشتل في عام 1971: «إن لك الحرية متى عُيِّنت في يوركتاون، أن تفعل ما تشاء، طالما كنت تقوم بعمل ما. ولقد أدّى فايشتل عملاً ـ إذ صاغ فكرة وضع نظام للكتابة بالشّيفرة».

إن الجانب الأكثر مدعاة للإعجاب في ما أبدعه فايشتل، لا يتصل بالرياضيات أو التكنولوجيا ـ أَو حتّى منعته أمام محلّلي الشّيفرة ـ بل الحافز الكامن وراءه. ذلك أنه لم يقصد بالشّيفرة المنيعة حماية أسرار الحكومة أَو المراسلات الدبلوماسية، بل أن صيانة خصوصيات الناس وأسرارهم ـ تحديداً قاعدة البيانات للمعلومات الشخصيَّة للأفراد من متطفلين قد يسرقون محتوياتها، ويستخدمونها لوضع ملفات شخصية مفصلة عن هؤلاء. وفي مقال لفايشتل نشره في مجلة سينتيفيك أمريكان Scientific American عام 1973 قال: «يشكل الكومبيوتر، أَو سوف يشكّل قريباً، تهديداً خطيراً لأسرار الناس

وخصوصيتهم. . . ولسوف يكون من الممكن قريباً جمع ملفات معمّقة عن كافة المواطنين». وأعلن أَن العلاج لذلك يكمن في الكريبتوجرافيا، وهي تقليدياً حكر على «العسكريين والدبلوماسيين». واقترح اعتماد أنماط من الكومبيوتر «توفر الحماية لمحتوياتها من الأيدي، إلاً أن يكون صاحبها مخولاً، عن طريق تشفير محتوياتها بأشكال شديدة المنعة على محاولات مفككي الشّيفرة». وهذا موقف هام لفايشتل، إذا أخذنا بعين الاعتبار معرفته بحرص الحكومة على احتكار المسؤوليّة. وقد ذهب فايشتل إِلىٰ الاعتقاد بأنَّه لما كانت السرية على قدر عظيم من الأهمية في عصر الكومبيوتر، فلا بد من الإعراض عن المقولات العصابية التي تتذرّع بدواعي حماية الأَمن القومي.

وفي غضون ذلك، كان فايشتل يبتدع نظاماً من شأنه أن يصون للناس أسرارهم وخصوصيتهم.

وأطلق على هذا النّظام اسم ديمن Demon (عفريت)، وسمي كذلك لأن ملف الأسماء في لغة الكومبيوتر الذي يستخدمه (أبي إل APL)، لا يتسع للكلمة الطويلة التي اختارها لتسمية النسخة الأولى من هذا النظام، فقد سمّاه ديمونستريشن (برهان، عرض) Demonstration. ثم قدر أن يقوم زميل له في شركة آي بي إم، بتغيير الاسم، ففي لحظة إبهام حول الموضوع الشيطاني من ديمن إِلىٰ لوسيفر Lucifer (إبليس)، مضمناً الكلمة تورية كريبتوجرافية من صميم الموضوع.

كان لوسيفر، من حيث هو مشفر بالجملة، آلة حقيقية، تمتص كتلاً من النصوص الواضحة، وتلفظها كتلاً من النصوص المشفرة. ولقد قام فايشتل بصنع عدةَ نماذج من هذا النمط؛ واستخدم في النموذج الأشهر مفتاحاً رقمياً Digital Key يتألَّف من 128 خانة ثنائية (بت Bit)، وهو هدف يصعب بلوغه بهجوم بالقوة الغاشمة. وصعب إِلىٰ حد الاستحالة. وغني عن القول، أن موضوع طول المفتاح لا ينطوي على أهمية كبرى إذا أمكن لمفكّك الشّيفرة

اقتحام النِّظام، باكتشاف نقاط الضعف في بنيته، واستغلالها فيستعيد النص الواضح دون أن يكلف نفسه شن هجوم بالقوة الغاشمة. ومحلِّل الشّيفرة يستطيع اقتحام النِّظام، إذا وجد في النص المشفر أدنى قدر من الانتظام. إن قوة لوسيفر شأنه في ذلك شأن أي شيفرة أخرى، تعتمد على منع الخصوم المحتملين من الوصول إلىٰ مثل هذه الطُّرق المختصرة. ولقد خلت الشيفرة التي ابتدعها فايشتل من التي تنبئ بأسرار النص لأنه أخضع ذلك النص إلىٰ جولة رياضية (حسابية) مضنية، تدور به في دوامة معقدة من الاستبدالات. وفي النهاية، وبعد ست عشرة «دورة» من التبادلات المحمومة مع الحروف الهجائية الأخرى، فإن كلمات النص والجمل تظهر ككتلة من حروف تبدو موضوعة بشكل عشوائي: أي نص مشفر بصورة غير مباشرة.

كانت قواعد الاستبدال الحاسمة يتم تنفيذها بوساطة صندوقين أَو (صندوقا ـ إس). ولم يكن هذان صندوقين بالمعنى المادي للكلمة، وإنما مجموعتان من المعادلات البيزنطية غير الخطية تحدِّد الطُّرق التي ينبغي بها تحريك الحروف. (يعتقد واحد على الأقل من زملاء فايشتل، هو آلان كونهايم، بأن وكالة الأَمن القومي هي التي قدَّمت له فكرة الصندوقين ـ إس، في ورشة عمل أقيمت ذات صيف لتوفير تكنولوجيا يفهمها القائمون على الأمور في فورت ميد، ومن ثم اعتمادها وتعميمها. ويقول كونهايم في هذا الصدد: «إن هورست رجل بالغ الذكاء، لكن أحسب أنَّه كان يتلقَّى توجيهاً وإرشاداً»).

إن الصندوقين ـ إس، لم يأتيا بمجموعة من الاستبدالات المنطقيَّة للحروف وحسب، بل كانا يستخدمان أيضاً معلومات مستقاة من مجموعة من الأرقام تؤلِّف مفتاحاً سرياً لتغيير السياق كلما مرت البتات عبر الصندوقين. وكان أمن النِّظام يعتمد، في النهاية، على هذا المفتاح. فبدون معرفة هذا المفتاح لن يستطيع عدو، ولو عرف كل القواعد التي يعمل بها لوسيفر، أن يحول النص المشفر إلىٰ نص واضح بأسلوب هندسي معاكس.

كان يفترض أن مثل هذه المعرفة بقوانين النِّظام متوفرة؛ وقد أُخذ في الاعتبار الاحتمال القوي بإمكانية معرفة المتنصت بتفصيلات الشيفرة التجارية الموزعة توزيعاً حسناً أكثر مما هو ممكن بالنسبة للشيفرة العسكرية التي يمكن إحكام السيطرة عليها بصورة أشد من الشّيفرة التجارية. ومحلّل الشّيفرة إذ يحاول تفكيك شيفرة عسكرية يفتقد في الغالب للمعرفة بالنظام المستخدم في وضع الشّيفرة؛ وتلك معضلة لا تقتضي توفر وقت طويل لتفكيك الشيفرة وحسب، بل معرفة واسعة بوسائل المخابرات السرِّيَّة أيضاً. وهناك شبكات تجسّس ضخمة، تكرّس جهودها لمعرفة أنواع الرموز التي يستخدمها العدو. ومن جهة أُخرى، إذا قرَّر بنك تشيس مانهاتن استخدام شيفرة آي بي إم لتشفير معاملاته المالية، فإن بوسع محتال أن يكتشف نظام التشفير الذي يستخدمه البنك. ولما كان ثمة احتمال بأن تجيز آي بي إم لأطراف أخرى استخدام هذا النِّظام، فإن قواعد العمل به تغدو على الأرجح متداولة على نحو واسع. وهكذا فإن السرِّيَّة كلها سوف تعتمد، في هذا العصر الجديد من التشفير غير العسكري، على المفتاح.

ولقد سعت شيفرة آي بي إم، إلىٰ امتلاك عدة براءات ملكية للوسيفر وحصلت عليها. وأصبح هذا النِّظام الذي ابتكر في مختبر واطسون للبحوث التابع للشركة من موضوعات البحث. ولكنَّه لم يكن يشبه المشاريع الخيالية السابقة لزمانها والتي كانت تجري في مختبر واطسون، إذ كان ابتكاراً يوفر حلاً فورياً لمشكلة راهنة ملحّة ـ أمن البيانات في عصر الاتِّصالات ـ وله موقع طبيعي على درب الاستثمار التجاري السريع. وسرعان ما تحقّق أول تطبيق جاد للوسيفر، في نظام نقطة الدفع، فبنك لويدز في لندن، اعتمده في توزيع العملة الصعبة على الزبائن. ولا ريب بأنه كان إيذاناً بقدوم أحداث أضخم لشركة آي بي إم والكريبتوجرافيا معاً. وكانت مسألة وقت وحسب، حتَّى يبلغ طفل هورست فايشتل نضجه، فلا يعود مجرد مشروع للبحث؛ بل سيغدو مبادرة كبرى من آي بي إم. ولسوف يغير هذا، المشهد كله.

بينما كان فايشتل منصرفاً لتشذيب وتطوير لوسيفر، كان هناك مهندس في الثانية والثلاثين من العمر، يدعى والتر تكمان، يعمل في فرع آي بي إم في كينجستون، في نيويورك. وكان هذا قد أصبح من الموظفين الدائمين في الشركة بعد أن عمل لديها خلال شهور الصيف الثلاثة من عام 1957، ما بين تخرّجه وتأديته الخدمة العسكرية. ولما انتهى من الخدمة الإلزامية، لم تقم آي بي إم بتوظيفه لديها مجدداً وحسب، بل أوفدته أيضاً إِلىٰ جامعة سيراكيوز لنيل شهادة الدكتوراه في نظرية المعلومات. وفي حين أن الغالبية من زملائه في الجامعة ظلّوا يتابعون العمل في الحقول الأكاديمية، فإن تكمان اتجه للاستفادة من معرفته في ابتكار تكنولوجيا متقدمة فعلاً، وكان أن لازم شركة آي بي إم، وانتهى بأن ترأس مجموعات الإنتاج.

كانت أحدث مهمّة يتولاها تكمان في الشركة، تتصل بضعف غريب في أمن الكومبيوتر، يتجلّى بتسرّب شارات إِلكترونية واهنة أثناء اتّصاله بأطراف أخرى وهذا ما يجعل متلصصاً حاذقاً، يستطيع استخدامها في إعادة بناء المعلومات التي تظهر على الشاشة. وبالنتيجة تمثّل هذه العلامات رصداً غير مشروع لبيانات سلك وصلة التفريغ في الكومبيوتر. وقد طلبت الحكومة ابتكار أداة خاصة توفر لحواسبها الوقاية من هذه التسرّبات الممكنة الوقوع، فاستجابت آي بي إم لهذا الطلب، بابتكار ما أصبح يُعرف باسم تكنولوجيا تمبيست Tempest (العاصفة). واعتبر هذا الابتكار فوزاً عظيماً، وحين أنهت مجموعة تكمان عملها عام 1971، شاء أعضاؤها الاستمرار في العمل معاً، عوضاً عن توزعهم بين مشاريع مختلفة، وفق الإجراء المعروف داخل الشركة بكلمة التشتيت الألمانية Volkerwanderung. ولكي يحصل ما يريدونه، كانوا بحاجة إِلىٰ مهمّة جديدة. وكان رئيس تكمان يعلم أن ثمة أموراً مثيرة للاهتمام تجري في قسم العمليات المصرفية، وربما تتطلّب تطويراً وابتكاراً في مجال أمن الكومبيوتر، فاقترح أن يتولى تكمان وفريقه النظر في الموضوع.

ولقد صادف أن موقع قسم العمليات المصرفية في الشركة، كان على الطرف المقابل لمكتب تكمان في كينجستون. وسرعان ما اكتشف تكمان أن رئيسه أصاب، حين استجاب لما أملته عليه الغريزة، فبعث به إِلىٰ ذلك القسم. وكانت الشركة قد قرّرت بناء على تجربتها في مشروع مصرف لويدز، طرح فكرة كوى للسحب الآلي، حيث يستطيع زبائن المصرف سحب الأموال من حساباتهم دون الاضطرار لمقابلة موظف. وكانت أولى آلات السحب خزائن ضخمة لا تحتوي على الأموال فقط، بل كذلك على كافة الأَجهزة الإِلكترونية والكومبيوتر، اللازمة لعملية الصرف والسحب، وهي عمليَّة مكلفة وصعبة. وكان الحل الأفضل، نشر البرنامج التطبيقي بين الكوة والكومبيوتر الرئيس في البنك، الذي يتولّى كافة المعالجات المعقَّدة. ولم يكن هذا الحل ناجعاً وحسب، وإنما يتفق بعد ما أدركت شركة آي بي إم حديثاً، أن مآل النموذج الأساسي للكومبيوتر سوف يكون مقابر الخردة. ويشرح تكمان ذلك بقوله: «كانت معالجة المعلومات تتم داخل الكومبيوتر الرئيس. وكان الأَمن النموذجي يقوم على أن تقفل باب غرفة مكتبك، بعد أن تقفل الإدراج، وأن يتولى حراسة المبنى رجل مسلح بمسدس. أما الآن، فإن أشد الناس التزاماً بالتقاليد في أرمونك يدرك أن معالجة المعلومات سوف تجري مستقبلاً خارج المبنى». وبما أنَّ الحارس المسلح يمكنه التواجد في كل مكان، فلا بدّ من تغيير هذا النموذج من الأَمن.

إن نظاماً يضخ المال فعلاً لكفيل بأن يمثّل تحدياً جدياً لأي نمط جديد من التجهيزات الأمنية لدى آي بي إم. فالأوامر الحاسمة التي تضيء الشارة الخضراء للفظ الأوراق النقديَّة من فئة العشرين دولاراً، سوف توجه مستقبلاً عبر خط الهاتف. وقد أدرك تكمان بسرعة مبلغ خطورة هذا الأمر. تخيل أن محتالاً عارفاً بالتكنولوجيا استطاع دخول خط الهاتف وتمكّن من تقليد الرسائل التي توجّه الأمر بـ «ارم فئة العشرين دولاراً!».

وكان العلاج هو الكريبتوجرافيا. ومع أن تكمان درس نظرية المعلومات، فإنَّه لم يسبق له أن قام بأي عمل في مجال الشّيفرة. لكنه سرعان ما اكتشف أمر النِّظام الذي ابتكره الباحثون في مركز البحوث في شركة آي بي إم في يوركتاون هايتس. وفي أحد الأيام، قام بزيارة مختبر واطسون، وسمع هناك فايشتل يتحدث عن لوسيفر. وللتو، دعا كلاًّ من فايشتل وآلان كونهايم إلىٰ الغداء. وكان أول ما فعله يومئذ سؤال فايشتل عن المصدر الذي استقى منه الأفكار لمشروع لوسيفر. فذكر له فايشتل، بلكنته الألمانية المميزة، دراسات كلود شانون المبكرة قائلاً: «إن أوراق شانون تبين الأمر كله».

وفي غضون ذلك، كان زميل تكمان، كارل ماير يبحث فيما إذا كان لوسيفر يصلح لأن يكون نسخة موسعة للنظام المستخدَم في كوى الدفع (الصرّاف الآلي) في بنك لويدز. وخلص تكمان في النهاية إلىٰ أن لوسيفر قد يحتاج على الأرجح إلىٰ عدد من التعديلات قبل أن تتوفَّر له المنعة الكافية، بحيث يمكن الاعتماد عليه. لكنه يصلح الآن ليكون بداية جيدة. وهكذا تم الاتفاق بين آلان كونهايم، ومجموعة نظرية المعلومات على أن يتولّى تكمان وفريق ماير في كينجستون، وضع خوارزمية منقَّحة للوسيفر وإرسالها من ثم إلىٰ يوركتاون لتقويمها واختبارها.

كان الاسم الذي عُرفت به الشّيفرة هو: دي إس دي ـ 1 DSD-1، قبل الموافقة على هذا الترتيب سأل أحد كبار المدراء في آي بي إم، عمّا يحمل هؤلاء الباحثين على الانشغال بلوسيفر، وهو يعرف أن ثمة خوارزمية أقلّ كلفة وأسرع عملاً. فقام تكمان بأخذ هذه الخوارزمية التي يفترض بأنَّها الأفضل إلىٰ بيته، وفكّكها أثناء العطلة الأسبوعية. (وكان أن نشر وماير عملية التحليل في مجلة التجارة داتاميشن Datamation. ومنذ ذلك الحين، دأب تكمان على الإشارة إلىٰ هذا النصر بوصفه برهاناً على معرفة فريقه بما يفعلون ـ وليضمن عدم توقف العمل نتيجة تدخلات لا سند لها من المعرفة من المدراء في الطوابق

العليا. ويذكر أنَّه قال ذات مرّة لأحد المتسلطين الكبار، هؤلاء الذين يمسكون بلقمة العيش: «إننا لا نستطيع التعامل مع هواة في الحقل. وليس هناك من طريقة رخيصة للقفز فوق خوارزمية الشيفرة. بل عليك أن تعمل وتعمل وتثابر على العمل، ثم أن تدقِّق وتمحّص وأن تكون مؤهلاً لذلك، ولسوف يستغرق هذا وقتاً طويلاً».

وكانت هذه عملية صعبة إِلىٰ حد بعيد ـ كما كان يمكن لهويت ديفي أن يقول لمجموعة كينجستون ـ وذلك بسبب الافتقار للمعلومات اللازمة لتصميم نظام تشفير حديث له قوة نظام التشفير العسكري. وفي ذلك قال تكمان متنهداً: «كان هذا كله من الأسرار المحظور الإِطلاع عليها. بيد أننا استوعبنا من دروس الرياضيَّات السرّ الذي يجعل شيفرة ما عصية على الحل». ولقد قرأ أعضاء فريق العمل كل ما في المكتبة، لكن كان أكثر ما وقع بين أيديهم فائدة وعوناً هو، كما تنبأ فايشتل، أبحاث شانون. ثم محاوراتهم مع فايشتل ذاته. بيد أن أكثر ما شُغلوا به كان إعادة اكتشاف ما يعتبر من المعارف الشائعة لدى نساج الخوارزميات في فورت جورج ميد. ويقول تكمان: «كنا نجلس في غرف الاجتماعات، وننشغل بالكتابة على السبورة ونعلِّم أنفسنا».

وسيكون الوضع مثالياً لو أمكن انتقال فايشتل إِلىٰ كينجستون، وضمه إِلىٰ الفريق. ولذلك، لم ينقطع تكمان عن سؤال كونهايم: «ماذا يريد هورست أن يفعل؟ لسوف أوفر له غرفة مكتب جيدة خاصة به، وله أن ينتقل إِلىٰ هنا». وكان كونهايم يجيب: «لا، لا أعتقد أن هذا الترتيب سيكون له حظ من النجاح».

وأخيراً؛ أدرك تكمان السَّبب. وقد قال فيما بعد: «كان هورست نسخة أوروبيّة عن جيمس ستيوارت في فيلم «هارفي»، كائناً يعيش في عالم سحري صغير، موزعاً بين ما يجري في مؤسَّسة تجارية مثل آي بي إم، وهواياته. إنني لم أشعر أن هورست كان يفهم حقيقة عالم التجارة والمال ـ وخاصة عالم

التجارة في التكنولوجيا المتقدمة. كان يعيش معتكفاً، منكباً على البحث في يوركتاون، بينما كنا، نحن المجانين من كينجستون، المستعدين فعلاً لصنع منتجات، نبحث إن كان بوسعنا أن نقوم بشيء يأتي بالمال».

يوافق كونهايم على أن فايشتل كان في غير محله، في عالم التجارة، بل يتبيَّن له مع مرور الزمن، أنَّه في غير موضعه في قسم البحوث من ذلك العالم أيضاً. ويروي كونهايم أن فايشتل اعتاد، منذ أن أصبح لوسيفر يبتعد عنه كاختراع له، ويزداد بروزاً كمنتج تجاري من آي بي إم، التأخّر في الوصول إلىٰ مكتبه في يوركتاون، فلا يعمل في مشروعه، بل يمضي سحابة يومه في إجراء المكالمات الهاتفية، بالألمانية. ويذكر كونهايم أن عمة فايشتل العجوز وعدته بإرث كبير، فكان يمضي الكثير من الوقت في التحدّث معها بالهاتف لاسترضائها. (أصيب فايشتل بخيبة أمل مريرة، والعهدة على كونهايم حين توفيت العمة بعد سنوات عديدة دون أن تخلف له شيئاً).

يعتبر المقال الذي نشره فايشتل في مجلة سينتيفيك أمريكان عام 1973، واحداً من أكثر الوصوفات العلمية، للكتابة بالشّيفرة وضوحاً، التي عرضت للجمهور منذ سنين ـ ويمكن تفسيره بأنَّه ضرب من التمرّد. وبالتأكيد، أن مثل هذه الصراحة التي تناول فيها المقال الخفايا الكريبتوجرافية لمادة تعتزم شركة آي بي إم إنتاجها كان حرياً بها أن تثير في بعض الأوساط، أكثر من مجرد الاستغراب. فقد اعترضت وكالة الأَمن القومي ذاتها، على ما يبدو، على نشر المقال؛ وأشار فايشتل إلىٰ ضيق الوكالة بالمقال، ملاحظاً أيضاً أنَّها كانت ستسعى لإسدال الستار على مشروع لوسيفر برمته، كما سبق أن فعلت مع مشاريع أخرى له، لولا فضيحة ووترجيت يومذاك التي قلبت واشنطن عاليها سافلها.

أما مجموعة كينجستون، فكانت لاهية عن مثل تلك المؤامرات. فقد كان الأمر بالنسبة لهم، أن لوسيفر مجرد مَنتَج قيد التطوير. فعملوا على التركيز على

هدف تعديل النظام وزيادة تعقيده، وصعوبته، بحيث يتمكَّن النص المشفر الصادر عنه من اجتياز اختبارات شانون لعشوائية المعلومات الظاهرة. وكانت أول خطوة وضع قائمة بما أطلقوا عليه اسم استكشاف المؤهلات، وهي سلسلة من الاختبارات الرياضيَّة التي تقيِّم مخرجات نظام الشّيفرة ـ الرسالة المعماة ـ بحيث لا تحمل علاقة ظاهرة بالرسالة الأصلية، فتبدو كمجموعة من الحروف المرتبة عشوائياً. وتكون محصلة محتوى المعلومات الظاهرة، في مصطلح كلود شانون صفراً.

من المؤكد أن نسخة فايشتل من لوسيفر، حاولت أن تبلغ هذا الوضع المثالي، لكنَّها ظلَّت دون هذا الهدف المنشود. وكان أقوى مكوناته صندوق ـ إس، حيث تتم أعقد الاستبدالات، أي التحولات اللاخطية المصمّمة لدفع محللي الشّيفرة إِلىٰ الجنون. فقرَّرت مجموعة كينجستون تزويد النموذج الجديد المطور من لوسيفر دي اس دي ـ 1، بصناديق استبدال أشد مراوغة ودهاء. وتقرّر زيادة عددها من اثنين كما في لوسيفر إِلىٰ ثمانية.

وزاد من تعقيد ذلك الجهد، ما طلب توفيره في النسخة الجديدة، وهو أن تكون مدمجة وسريعة. فكان المطلوب على حد تعبير تكمان، أن تكون هذه النسخة «زهيدة الثمن وسريعة». ولتوفير هذه المتطلبات كان ينبغي استيعاب الخوارزمية كلها في رقاقة chip واحدة. وهكذا تم توزيع جزء آخر من الفريق، ويعرف باسم مجموعة ڤي إل إس آي VLSI، اختصاراً لـ Very Large Scale Intergration الدمج/ التكامل الواسع النطاق، بين مختبرات كينجستون وآي بي إم في بيرلنجتون بولاية فيرمونت، وقد أنيطت بهذه المجموعة مهمّة وضع نظام التشفير كلّه في رقاقة واحدة بحجم 3 ميكرون. وكان من المقدَّر أن تخرج الشركة ـ إن سارت الأمور على ما يرام ـ بأصغر وأقوى آلة تشفير عرفها العالم.

ولقد قدَّم فريق كينجستون وهو يعمل ضمن هذه الشروط، نسخة دي إس دي ـ 1 المعقَّدة، والتي ما زال يُشار إليها حتى ذلك الحين باسم: لوسيفر. وكان مقدراً، إن سارت الأمور جيداً، أن يستوعب لوسيفر الجديد كتلة من نص واضح يتألَّف من 64 بت، ثم يعالجها عبر عملية مضنية من تغيير مواقع الحروف والتكتيل، والتوسيع، والربط، والاستبدال الذي يعتمد على مفتاح رقمي Digital Key، ثم تكرار العمليَّة خمس عشرة مرة أخرى، ليكون المجموع ست عشرة دورة. وتكون المحصلة 64 بت، مما يبدو ضرباً من فوضى رقمية، حشد لا يمكن أن يعود للانتظام، إلاَّ بواسطة شخص يقوم بعكس عملية التشفير باستخدام المفتاح الرقمي الذي حدَّد الكيفية التي تمّت بها عمليَّة التعمية بخلط الحروف.

وبعد هذا، كان فريق مختبر واطسون يتولَّى محاولة القيام بالهجوم للتحقّق من سلامة العمليَّة برمتها.

ومع أن هورست فايشتل، لم يكن معنياً ببناء النموذج دي إس دي ـ 1، فقد ساعد زملاءه في البحث على تسريع عملية الاختبار. وفي 11 كانون الثاني/ يناير 1973، جمع فايشتل خمسة من زملائه في مجموعة أمن البيانات في يوركتاون هايتس، وعرفهم لأول مرة على شيفرة لوسيفر. وقد أثار أحد أعضاء المجموعة، وهو ألان تريتر (عالم الكمبيوتر الغريب الأطوار ذاته الذي عرَّف هويت ديفي إلىٰ أصول نظام التحقّق من الصديق أَو العدو آي إف إف) شكوكاً حول جدوى المشروع برمته. فهل تريد شركة آي بي إم أن تجازف بوضع نفسها في خطر، في محاولتها أن تكون قوة في عالم الكريبتوجرافيا التجارية الجديدة؟ وماذا لو أمكن تحطيم شيفرة لوسيفر؟

أثارت هذه الملاحظات التي أبداها تريتر الاهتمام، إذ بدت صدى لبعض الملاحظات التي أوردها أحد الأساتذة في جامعة كيس ويسترن ريزيرف،

ويدعى إدوارد جلاسر، وإن لم يأت بدليل على صحتها. فهذا الرجل الكفيف، وهو واحد من سلسلة لا حصر لها من المستشارين الذين توظفهم شركة آي بي إم بميزانيتها غير المحدودة، ادعى حسب رواية كونهايم، بأنَّه لو أعطي عشرين نموذجاً من نصوص مشفَّرة مع النص الأصلي الواضح (وهو ما يُعرف بالهجوم على نص واضح منتقى) لاستطاع تفكيك نظام لوسيفر. (تبين فيما بعد أن ذلك زعم خادع مقبول في ظاهره وحسب).

لكن الفكرة فهمت على نحو جيد، وقد كرّرها تريتر في مذكرة وضعها في وقت لاحق من ذلك العام. فكتب فيها: «قد كنا/ نحن في وضع مكشوف على نحو غير مألوف». وأبرز في ملاحظته حول استخدام لوسيفر لأول مرة في كوة الصرف في بنك لويدز، العواقب المترتبة إذا ما ترك النظام مكشوفاً على نحو ما، شأنه في ذلك شأن الكثير من الأنظمة التي سبقته والتي كانت تبدو «منيعة». وكتب في ذلك يقول: «إذا استطاع شخص ما إنتاج مفتاحٍ يصلح لشيفرة لوسيفر، فلسوف يقيض له النجاح بالتأكيد إن قام بمحاولة ذكية وحسنة الإعداد ودون استخدام القوة بتفريغ كافة كوى الصرف الآلي للنقود من محتوياتها أثناء العطلة الأسبوعية».

أثارت هذه الملاحظات التي أبداها تريتر الاهتمام، إذ بدت صدى لبعض الملاحظات التي أوردها أحد الأساتذة في جامعة كيس ويسترن ريزيرف،
ويدعى إدوارد جلاسر، وإن لم يأت بدليل على صحتها. فهذا الرجل الكفيف، وهو واحد من سلسلة لا حصر لها من المستشارين الذين توظفهم شركة آي بي إم بميزانيتها غير المحدودة، ادَّعى حسب رواية كونهايم، بأنَّه لو أعطي عشرين نموذجاً من نصوص مشفَّرة مع النَّصّ الأصلي الواضح (وهو ما يُعرف بالهجوم على نص واضح منتقى) لاستطاع تفكيك نظام لوسيفر. (تبين فيما بعد أن ذلك زعم خادع مقبول في ظاهره وحسب).

إلاّ أن مثل هذه الخسارة، إنما كانت بداية ذلك النوع من المخاطر التي تواجه شركة آي بي إم بأخذها بالوعد الضمني بالأمن الذي حملته الكتابة بالشّيفرة. وليست المشكلة هنا في التعويض لبنك لويدز عن خسارته، ولو بلغت أَكداساً من فئة العشرين دولاراً، فذلك في استطاعة الشركة العملاقة، بما لديها من احتياطي ضخم من النقد. فالأَدعى للقلق هو استعادة ثقة الناس متى فقدت. ثم هناك، بعد، الدعاوى والمحاكم.

ولقد كتب تريتر: «لو قدر انتهاك أمن [لوسيفر] أَو أي منتج مشفَّر قد نطرحه لاحقاً [للتداول]، وذاع السر، فإن الضرر الذي سوف يلحقه بنا هذا الأمر في السوق يفوق الحصر. فضلاً عن الأضرار الفعليَّة والاحتمال الماثل بدفع تعويضات ضخمة، بقرار من المحكمة بعد الادعاء والمقاضاة في قضية ستكون الشغل الشاغل للصحافة والصناعة والجمهور».

ومن جهة أخرى، يبرز السؤال: هل بوسع شركة آي بي إم صرف النظر عن متابعة الكريبتوجرافيا؟ لقد كان عملها عصر المعلومات، وليس بوسع الشركة تسويق مثل هذا العدد الكبير من الكومبيوتر، إن لم توفر وسيلة لحماية البيانات وهي تنتقل من كومبيوتر إِلىٰ آخر. وإذن، فإن الافتقار إِلىٰ الكريبتوجرافيا، يشكل عقبة يحسب حسابها أمام تعميم الكومبيوتر أمريكيّاً، والعالم ذاته. فتم عقد اجتماع على مستوى عالٍ في 5 شباط/ فبراير عام 1973، لمراجعة «أحوال الكريبتوجرافيا والخطط الموضوعة لأجلها، داخل شركة آي بي إم برمتها». وكما قال تريتر في تلخيص ما تمّ في الاجتماع فيما بعد: «بدا أن ثمَّة اتفاق عريض... على أن آي بي إم غدت ملتزمة إِلىٰ الأبد بموضوع الشّيفرة، ولا بدَّ لها من امتلاك الخبرة من عدة حقول في هذا المجال. وفي الوقت ذاته، فإن الهجوم على لوسيفر سيكون أكثر حدَّة.

ولقد جرى ضم خبير من خارج الحلقة هو جيم سيمونز، الأستاذ بقسم الرياضيات في جامعة نيويورك في ستوني بروك، وكان قد مارس الكريبتوجرافيا في معهد تحليل الدفاع، التابع لوكالة الأَمن القومي في جامعة برنستون، للقيام بهجوم مركَّز على لوسيفر لاختباره. فعمل يومئذ إِلىٰ جانب ثلاثة باحثين من يوركتاون هايتس طوال سبعة أسابيع من أواخر ربيع عام 1973. ولم يكن هذا العالم قد أصدر تقريره بعد، حين أخذ المعنيون في الشركة يشيعون الأخبار الطيبة، وهي أن سيمونز ورفاقه لم يتوصَّلوا إِلىٰ قهر لوسيفر.

كتب سيمونز في تقريره المؤرخ في 18 آب/ أغسطس 1973: «إن آلة لوسيفر أشد منعة مما قدرت أصلاً». لكنَّه مع ذلك، لم يمنح لوسيفر خاتم المصادقة عليه. وقد خلص سيمونز في هذا التقرير إِلىٰ القول: «يبدو من المستبعد أن يتمكّن طالبان في المرحلة الثانوية، من التغلّب على لوسيفر في إطار بحث في مادة العلوم. ولكن من جهة أخرى ليس لدينا ما يكفي من الدلائل للثقة بأن لوسيفر لن يلين تحت ضربات جيدة التنظيم والتسديد، يوجِّهها محلِّل شيفرة محترف». وكان القلق يساور سيمونز من إنه إذا وُضع لوسيفر، وهو في حالته الراهنة، للاستخدام في الأغراض التجارية، فمن المحتم تقريباً استخدامه لحماية «نقل أشياء ذات أهمية حقيقية» (مثل المال والأسرار المهنية)، وهذا ما يوفِّر الحافز للقيام بجهد لا بدَّ وأن ينجح في النهاية لاختراقه. وهكذا، فإن لوسيفر، إن بدا لـ آي بي إم بداية طيبةٍ، فإن على الشركة، كما قال سيمونز محذراً أن تجهد أكثر لتخرج بنتاج محسَّن. وخلص في تقريره إِلىٰ القول: «الواقع أنَّه ليس ثمة خيار آخر».

وفي غضون ذلك ظلَّت الشركة تتساءل، إن كان لوسيفر سيصمد أمام

الامتحان. ففي مذكرة سرية صدرت في شهر أيار/ مايو 1973، شدّد كبير العلماء لويس برانسكومب، وهو يلخص إجماع اللجنة الاستشارية العلمية، على ضرورة قيام الشركة بـ «إرساء بنية كريبتوجرافية، وتكنولوجية، واستراتيجيَّة إنتاج موحّدة». وكتب، إن لوسيفر ليس بالمرشح الوحيد في هذا. ولكنَّه اعتبر في مذكرة أخرى أن خطة مجموعة كينجستون هي الأفضل، مع تحذير واحد: «إلاَّ أن يكون ثمة دليل واضح على وجود ضعف ذي أهمية».

استمرت الاختبارات عدة شهور، وكان يقوم بها باحثون من القطاع الخاص بتكليف من الشركة. ويصف تكمان ذلك بقوله: «كان ألان يقدم لهم الخوارزمية، قائلاً: «هيا فككوها! كل ما أطلبه منكم تفكيكها وحسب». ولا ينقطع عن القول، وهو يعود ليقدِّم تقريره: ما من أحد استطاع أن يجد فيها ثغرة. وأخيراً وصلت إِلىٰ النقطة السيكولوجية السحريَّة، ورأيت أن هذه الآلة لا تعاني من أي ضعف، وإذن، فليس ثمَّة حل مختصر لتفكيكها. وقلت للباحثين: دعكم من هذا يا شباب، ولنركِّز على تطبيق هذا المنتج الآن».

ومع ذلك، فإن معظم أساتذة الرياضيَّات الذين كانوا يتلقّون رواتبهم ليناطحوا لوسيفر يعتبرون هواة بالمقارنة مع محلّلي الشيفرة العالميين خلف السور الثلاثي. فكيف يمكن للشركة الوثوق بسلامة الخطة فعلاً؟ فالشركة ما كانت بالتأكيد راغبةً في معرفة نقاط ضعف لوسيفر، ثم أن تكتشف ذات يوم أن محلّل شيفرة كان يعمل في المخابرات السوفيتية كي جي بي سابقاً، ويعمل لصالح المافيا حالياً قد استطاع تنظيف خزائنها من النقود.

في بداية عام 1974 قدر تكمان أن فريقه قطع نصف الشوط من العمل. وفي هذا يقول: «كانت لدينا فكرة جيدة عن كمية الخوارزمية التي يمكن تحميلها لرقاقة واحدة». وكان معظم هذه الخوارزمية قد تمّت كتابته. ولكن حدث في ذلك العام أمران كان لهما الأثر العميق على المشروع. الأول جعل

هذا المشروع علنياً وطرحه على الملأ، والثاني ألقى عليه ظلاً خفياً من الشك، قدّر له أن يستمر جيلاً من الزمن.

لم تكن آي بي إم المؤسَّسة الوحيدة التي أدركت الحاجة الماسَّة للحماية الكريبتوجرافية في عصر الكومبيوتر. فقد كان يشاركها هذه النظرة المكتب القومي للمعايير، وهو الوكالة الحكومية التي تتولّى وضع المعايير الصناعية التجارية. فقد كان البيروقراطيون والعلماء هناك يعتقدون بضرورة تركيز الحماية الرقمية في نظام واحد، أحسن اختباره في تشفير المعلومات، ويمكن للناس كافة استخدامه. ولذلك قرَّر المكتب القومي للمعايير طلب خوارزمية تشفير قياسية. (رفضت وكالة الأَمن القومي تقديم إحدى الشيفرات التي تستخدمها خوفاً من اطلاع الغرباء عليها، وهذا من المحرمات التي لا يمكن التفكير في انتهاكها). وفي 15 أيار/ مايو 1973، نشر المكتب القومي للمعايير في مجلة فيدرال ريجيستر، عدداً من المعايير الدقيقة التي ينبغي توفّرها في هذه الخوارزمية القياسيَّة.

ولم يكن مفاجئاً، أن المكتب القومي للمعايير، لم يتلق في ذلك الحين أية عروض تلبي تلك المعايير المطلوبة، ولو بشكل مبهم. ذلك أن معظم المختصين بالكريبتوجرافيا، والوحيدين الذين لديهم المقدرة والخبرة لقبول هذا التحدي، كانوا يعملون خلف السياج الثلاثي، وكانت بحوثهم التي يجرونها هناك لا تنشر ولا يكشف عنها.

ومع ذلك، فقد كان ثمة نظام تشفير واحد قيد التطوير بدا ملبياً للكثير من احتياجات الحكومة، هو لوسيفر دي إس دي ـ 1. ورأى لويس برانسكومب، كبير العلماء لدى آي بي إم ـ وكان هو نفسه، وليس من قبيل المصادفة، رئيساً سابقاً للمكتب القومي للمعايير ـ على وجه الخصوص، أن هذا العمل الذي يجري تطويره، يمتلك المقومات اللازمة لمعيار التشفير اللازم للجيل القادم.

كان والت تكمان مناهضاً لهذا الرأي بسبب المقايضة التي ينطوي عليها طرح لوسيفر المعدل كمعيار فيدرالي، إذ يقتضي أن تتنازل الشركة عن حقوق الملكية الفكرية، وهذا يعني بالضرورة تقديم الخوارزمية ـ وليس بيعها ـ للعالم. وفي هذا يقول: «كنت من هذا النمط النموذجي لمدير مبيعات رأسمالي. إنني أعمل في هذا المشروع لأجني المال، وليس لرعاية حركة اجتماعية عظيمة». وذلك ما عرضه تكمان أمام أحد كبار مدراء آي بي إم، بول ريزو، الذي كان يحتل يومئذ المنصب الثاني في أعلى السلم في الشركة العملاقة. كذلك عرض برانسكومب وجهة النظر الأخرى المتمثّلة في جعل الاختراع عاماً. وأخيراً تدخّل ريزو في النقاش الدائر، مشبهاً لوسيفر بعنصر أمان، فهو إذن مفيد للمجتمع كله. وكانت حجته هي: إذا استطاعت شركة فورد أن تنتج حزاماً للأمان أفضل مما لدى منافسيها، وفيه نجاة الأمهات والآباء، فهل كانوا سيسمحون لجنرال موتورز أن يستخدموه في سياراتهم؟ الأفضل أن تعتقد بأنّهم سيفعلون ذلك، لأنه رأي صائب. إن [الممثل الشهير بخطاباته المؤثرة] جيمس ستيوارت ما كان ليستطيع أن يأتي بموعظة أقوى من هذا البيان، ولقد كان بوسع المرء سماع الكمان وهو يعزف أعذب الألحان، حين انتهت الخطبة. ولم يقنع هذا الحديث مجلس إدارة الشركة وحسب، بل امتد أثره إِلىٰ تكمان ذاته، الذي دعا إِلىٰ اجتماع عند عودته إِلىٰ كينجستون، ليقول لجماعته «حسناً يا شباب، إننا سوف نتخلّى عن هذا الذي بين أيدينا».

ولم يكن معنى ذلك التخلي عنه كلياً، طبعاً. فالطرق التي استخدمت في تحويل لوسيفر إِلىٰ رقاقة، والأساليب التي سوف ينفذون بها الآلة في إطار حل كامل، والحيل الصغيرة التي تمكنهم من استغلالها إِلىٰ أقصى حد. . . هذه كلها، تشكل مواد تجارية مربحة للنسخ التي ستبتكرها آي بي إم عن الأصل دي إس دي ـ 1. أما الشركات الأخرى، فلن يتاح لها إِلاّ الحصول على الخوارزمية

ذاتها. وإذن فرُبَّ ضارَّة نافعة، ولربما أتى التخلي عن الآلة وطرحها على الملأ بربح وفائدة، من وجهة النظر التجارية.

كان الشعور السائد في شركة آي بي إم، أن مجرد تسليم صنيعتها للمكتب القومي للمعايير، كان كافياً لتتويج دي إس دي ـ 1، كمعيار ومثل يُحتذى. ومع أن الموعد المحدّد لتقديم الاستجابة لطلب المكتب القومي للمعايير تقديم عروض لخوارزميات تشفير في عام 1973 قد انتهى، قبل فترة طويلة، فقد كتب برانسكومب لخليفته في المكتب القومي للمعايير، روث ديڤيس في تموز/ يوليو 1974 يعرض ما وصفه بـ «خوارزمية شيفرة بمفتاح تحكّم» تم تطويره في لينجستون. ولما وجد المكتب هذا المرشح الجديد الأثير مطروحاً للمنافسة، كرّر الإعلان عن طلب عروض لخوارزميات تشفير، وقد نشر هذا الإعلان في مجلة فيدرال ريجيستر، بتاريخ 27 آب/ أغسطس 1974. ولم يبرز يومئذ أي منافس. وهكذا قدر للوسيفر المعدل دي إس دي ـ 1، أن يعرف باسم جليل وإن كان ينم عن أصله معيار تشفير البيانات Data Encryption Standard. ولقد غدا هذا الاسم معروفاً بين الراسخين في علم الأَرقام، حتَّى أنَّهم لم يأخذوا باسمه المركب الكامل، بل شرعوا يشيرون إليه بلفظ مختصر: ديز Dez.

وفي ذلك الوقت، كان ثمة تطوير دقيق آخر يتصل بتحول لوسيفر. وجرى ذلك في بدايات عام 1974 حينما تلقَّى والت تكمان ما صار يصفه لاحقاً بـ «تلك المكالمة الهاتفيَّة القاتلة». وكان المتحدِّث رئيسه، الذي أخبره بأنَّه مضطر للقيام برحلة إِلىٰ مقر وكالة الأَمن القومي لتهدئة خواطر القوم هناك، مما أثاره لوسيفر بينهم.

لم يجد تكمان في هذا الحديث ما يطمئن فؤاده. لكنَّه أدرك أهمية مسايرة العم سام (الحكومة الأمريكية). فالحق أن شركة آي بي إم كانت تدخل بإنتاجها مادة تريبتوجرافية للقطاع التجاري أرضاً غريبة. وإذا لم تنل إجازة التصدير اللازمة لإرسال رقاقة الشيفرة إِلىٰ الزبائن في مختلف أرجاء العالم، فالأجدر

عندئذ صرف النظر عن هذه الصناعة. فما هي الفائدة من منتج لشركة عالمية مثل آي بي إم تشمل عملياتها الكرة الأرضية، إن لم تستطع بيعه في السوق العالمية؟

ولذلك مضى تكمان ليقوم بأول زيارة له إلىٰ فورت ميد. وتأمل بعينيه السياج الثلاثي وأفراد الحرس من مشاة البحرية، ثم أوقف سيارته في المكان المخصص للزائرين، ودخل المبنى الصغير المشيد بالإسمنت المسلَّح، حيث على الغرباء الذين لا يحملون إذناً مسبقاً بالزيارة، ملء كمية من الأوراق ثم الانتظار لاستدعائهم. وبعدئذ جاءته سيدة متقدمة في السِّن وسارت به في متاهة من الممرَّات ليصل إلىٰ أحد المدراء من المرتبة الثانية هو المكلف بالقضية، ويأتي بعد نائب المدير مباشرة. ولم يكن الرجل يرتدي اللباس العسكري أَو حتَّى بذلة رسمية. وأسرع يعرض اتفاقية بالمقايضة: إننا نريد أن تكون لنا السيطرة على تنفيذ هذا النظام. أنتم تقومون بتطويره سراً، ونحن نتابع عملكم ونقترح التغييرات. إننا لا نريد أن يتم تسويقه في برمجيات مشفَّرة، بل في رقاقات وحسب. ثم إننا لا نريد أن يصدر إلىٰ بلدان معينة على الإطلاق، ولسوف نسمح لكم بتصديره إلىٰ البلدان الواردة أسماؤها على قائمة إجازات التصدير فقط، إذا ما حصلتم على رخصة التصدير. ومنح تلك الإجازة مشروط بتوقيع الزبائن الذين نوافق عليهم على تعهد بعدم إعادة تصدير المنتج إلىٰ أي طرف آخر.

استمر الكلام على هذا المنوال لفترة من الوقت، حتَّى أتيحت لتكمان الفرصة للرد. فسأل ممثِّل الوكالة، وقد وجده يحصر حديثه بالممنوعات والمحظورات والشروط، وأهمل الحديث عما ستناله آي بي إم مقابل جهودها: «وهذا مقابل ماذا؟» أجاب رجل وكالة الأَمن القومي: «ستنالون بالمقابل شيئاً مفيداً جداً». وكان التعويض قيام الوكالة بإجازة الخوارزمية، بأن يقوم محلّلو الشّيفرة الألمعيون فيها بتحليلها واختبارها، فإذا لمسوا ضعفاً، رصدوه، ثم

عمدوا إلىٰ تقويمه. وعندما تمضي الزوبعة الرياضيَّة تنال الشركة إجازة لا تُقدَّر بثمن، ترخيصاً يكفل نيل ثقة الزبائن: خاتم المصادقة من وكالة الأَمن القومي بأن السرّ في الحفظ والصون.

كان هذا عرضاً قوياً، لأنه يتوجّه إلىٰ أقوى مخاوف تكمان مباشرة ـ وهو إمكانية اكتشاف محلّلي الشّيفرة الخارجين عن القانون حلاً مختصراً يسمح لهم باعتراض أسرار الزبائن، بل وسلب أموالهم أيضاً، وبذلك يعرّضون الشركة العملاقة ذات الشهرة الأسطورية لحرج على نطاق عالمي، ومجزرة قضائية. وهكذا، عوضاً عن اضطرار الشركة للاعتماد على الهواة النابهين. قليلي الخبرة، في يوركتاون والمشاورين الذين تستخدمهم كيفما اتّفق، ها هي ذي يعرض عليها امتلاك منتهى التدقيق والتمحيص: المعيار الذهبي في تحليل النصوص المشفَّرة. فكان أول ما قام به تكمان فور عودته من فورت ميد مقابلة رئيسه، ليحثّه على «قبول العرض والعمل مع هؤلاء القوم». وكان ذلك حلاً طابت له النفوس في أعلى المراتب، وهم في المقام الأخير مرادفون «للمؤسَّسة» [الحاكمة]. وهكذا غدا الجهد المنفرد الأهم الذي ينهض به القطاع الخاص في الكريبتوجرافيا في البلاد، لم يكن سوى ذلك العمل الذي كان يقوم به هويت ديفي، وهو ما يزال مغموراً، بعد، ويعارك أفكاره الغريبة في جامعة ستانفورد، ومحورها التوابع الوحيدة الاتجاه، في القبضة الودود، لكن الحازمة، لوكالة الأَمن القومي.

كان الأمر المقلق الذي ساور الباحثين يومذاك، احتمال اكتشاف وكالة الأَمن القومي ـ وهي ليست، ذراعاً لوزارة التجارة، بل وكالة استخبارات، وقصر أشباحٍ مطلق ـ ضعفاً فاضحاً في معيار تشفير البيانات، ثم الصمت عنه، وهم مطمئنون ليقينهم بأنَّ بوسعهم استخدام هذا الدرب الميسّر في تفكيك الرسائل المعماة في شيفرة الشركة. ولقد أدرك تكمان المجازفة الكامنة في هذا الوضع. وأخذ يرصد الشارات على امتداد الشهور والأعوام التالية، فيما كان

تطور المشروع يأخذ مداه. وفي النهاية، غدا الرجل مطمئناً إِلىٰ سلامة نوايا الوكالة، وفي هذا يقول: «لو أنَّهم ضلَّلوني لنزلت القبر مخدوعاً». ولذلك كنت أرصد هؤلاء القوم وجهاً لوجه. إنني من هواة الأفلام، ولقد شاهدت من التمثيل الحسن والرديء. ولو خدعني جماعة الوكالة، لضلوا سبيل مهنتهم، وكان ينبغي عليهم الذهاب إِلىٰ هوليوود واحتراف التمثيل».

ومنذ تلك اللحظة أصبحت عملية تطوير معيار تشفير المعلومات ديز، تتم من الناحية العملية خلف السياج الثلاثي. ثم أصدرت الحكومة قراراً سرياً يكتم براءة اختراع هورست فايشتل للوسيفر المعروف باسم نظام مفتاح متنوِّع لمصفوفة شيفرة Variant Key Matrix Cipher System. وفي 17 نيسان/ أبريل 1974 بعث محامي شركة آي بي إم المكلَّف ببراءات الاختراعات بمذكرة إِلىٰ الفريق القائم على بحوث الشّيفرة في يوركتاون هايتس وكينجستون، أن فحوى القرار يحظر نشر البحوث في هذا الموضوع ومناقشته علناً بأي شكل، إِلاَّ بإذن خطي من مفوض براءات الاختراع. كان كل ما يحيط بالأمر سراً حتى وجود أمر السرِّيَّة ذاته يعتبر سراً، والحديث عنه جريمة خطيرة خطورة تسليم خوارزميات الشّيفرة لمسافر من مطار كينيدي. وإفشاء المعلومات عنه عرضاً دون قصد، كفيل بأن يغرم المرء 10000 دولار، أَو عقوبة السجن عامين، أَو كلا العقوبتين معاً، كما ورد في المذكرة. ولكن الأمر منح آي بي إم إذناً خاصاً بالكشف عن هذا الموضوع في نطاق ضيِّق لأشخاص مشهود لهم بالولاء والأمانة والحفاظ على الأسرار، من الموظفين في الشركة من أَو يعملون معها، وتقتضي مهماتهم المشاركة في تطوير أَو صناعة أَو استخدام المادة موضوع التفاهم». ولولا هذا الاستثناء، ما كان بوسع آي بي إم الاستمرار في جهدها هذا، بسبب الصعوبة الجلية في التعاون في مشروع ينطوي على المجازفة، بالتعرض لعقوبة السجن جراء الاعتراف بوجوده لشخص يتعاون وإيَّاها.

كانت متطلبات وكالة الأَمن القومي سرِّيَّة متشدِّدة بالغة الصرامة بما يخص تحليل معيار تشفير البيانات ديز. ولذلك فإن أي أمر ـ مطلق أمر ـ يلقي الضوء على عمل محلِّلي الشيفرة في فورت ميد، يعتبر من أعظم الكبائر، وكان الاتفاق المعقود بين الوكالة والشركة يرسم بوضوح حدود ما يمكن للعلماء في الشركة جمعه من المعلومات جرَّاء هذا التعاون بينهما. فقد فرض على الشركة الاقتصار على عدد محدود من العلماء، ممن يعملون في تقويم المشروع ومراحله، ووضع قوائم بأسماء هؤلاء الأشخاص دورياً. وكان الإحتكاك بين الأزرق الكبير Big Blue [شركة آي بي إم] والمتطفّل الكبير Big Snoop [وكالة الأَمن القومي] يقتصر على سلسلة من الاجتماعات التي يطّلع فيها الطرفان على تطورات العمل، وفق قواعد دقيقة مضبوطة مثل مسرحية كابولي يابانية: تقدم الآي بي إم المعلومات، بينما يقوم جماعة الوكالة لتقييمها بصمت. ولم يكن مسموحاً خوض المجتمعين في الأحاديث المطولة؛ وكان محظوراً على جماعة الوكالة «الخوض في مناقشات تقنية مع ممثلي الشركة تتصل بالمعلومات المعروضة». وقد جرت القاعدة على أن يعقد جماعة الوكالة جلسات تشريح بعد تلك اللقاءات لمعرفة ما إذا كان العلماء في آي بي إم قد وقفوا على معلومات أو أفادوا من تقنيات «ذات طبيعة حسَّاسة. فإذا كان الجواب بالإيجاب، اضطرت الشركة وبات عليها إبقاء تلك المعلومات طي السرِّيَّة.

كانت وكالة الأَمن القومي تعرف بالتأكيد ما لديها، وقد أبدت عناية خاصة بأسلوب اكتشفه الباحثون في الشركة، يشار إليه في مختبرات واطسون باسم: «الهجوم تي»، ثم بات يُعرف لاحقاً باسم «تحليل الشّيفرة التفاضلي». وهذه سلسلة معقَّدة من المعالجات الرياضية التي تتطلَّب الكثير من النصوص الواضحة المنتقاة (لا بد للمهاجم من أن تتوفَّر له مجموعات من المراسلات الأصلية والنصوص المشفَّرة بعد المعالجة، والقيام بمقارنتها ببعضها البعض). وكان الباحثون في مختبرات واطسون قد توصلوا في وقت ما من ذلك العام، إلىٰ أن

في شيفرة آي بي إم ضعفاً يجعلها عرضة في ظروف معينة للسقوط أمام الهجوم تي ـ فيمكن للعدو إذا ما شنّ هجوماً ناجحاً معرفة أجزاء من المفتاح. فكان أن قام فريق من الباحثين في آي بي إم بإعادة تصميم الصندوقين ـ إس، للحيلولة دون إتاحة الفرصة لنجاح هذا الهجوم؛ ولم يعد بوسع المهاجم أن يستفيد من الهجوم تي بشيء يُذكر.

ولقد انتاب جماعة وكالة الأَمن القومي ضيق شديد لسماع النبأ. إذ يبدو أن أمر الهجوم تي كان معروفاً ـ وسرّاً بالغ السرِّيَّة ـ وراء السياج الثلاثي. وللمرء أن يتخيَّل ضيق الوكالة، عندما وجدت أن فريق الشركة لم يكتف باكتشاف الخدعة (التي كانت الوكالة تستخدمها في كشف شيفرات الأعداء) وحسب، بل ابتكر مجموعة من مبادئ التصميم لمواجهتها أيضاً. ولم يحتمل جنود الشيفرة في فورت ميد احتمال تسرّب مثل هذه المعلومات إِلىٰ الكتابات العامة في هذا الحقل. وهكذا كان، أن شدَّدت الوكالة قيود السرِّيَّة حيال الشركة.

ويذكر تكمان: «لقد طلبوا منا وضع خاتم السرِّيَّة على كل وثائقنا. فعمدنا إِلىٰ ترقيم كل وثيقة ثم وضعها في خزائن آمنة مقفلة، لأَنَّها في عرف حكومة الولايات المتّحدة سرِّيَّة. وصدر الأمر أن نقوم بذلك. فقمت به».

كان دان كوبر سميث هو الرجل الذي قام على الأرجح، بمعظم العمل المتعلّق بالهجوم تي في آي بي إم، وقد ظلّ يمتنع عن الخوض في أمره، طوال عشرين عاماً. ولم يكشف هذا الرجل مبادئ تصميم الصندوق ـ إس، إلاّ في عام 1994، وبعد ما كان باحثون آخرون قد اكتشفوا الأمر ووصفوا الأسلوب قبل ذلك بزمن طويل، وبشكل مستقل عن آي بي إم. وفي مقال تقني نشرته مجلة آي بي إم ريسيرش جورنال، كتب كوبر سميث: «لقد تقرَّر بأن الكشف عن جوانب التصميم، كفيل بأن يعرض للملأ أسلوب تحليل الشّيفرة التفاضلي،

وهو أسلوب فعّال يمكن استخدامه في تحليل الكثير من الشيفرات. وهذا من شأنه إضعاف المزايا التي تتمتع بها الولايات المتّحدة في التنافس، وتتفوق فيها على بلدان أخرى في مجال الكريبتوجرافيا».

ولقد تحقّق لآي بي إم في النهاية الوصول إِلىٰ مبتغاها، أي الحصول على شهادة براءة صحية لمعيار تشفير البيانات ديز، من وكالة الأَمن القومي. (وكان هذا عاملاً هاماً ليضع المكتب القومي للمعايير خاتمة بالمصادقة على أن يكون معيار تشفير البيانات معياراً فيدرالياً). غير أن الشركة دفعت ثمناً غالياً لالتزامها بأمر وكالة الأَمن القومي، والإبقاء على مبادئ تصميم الصندوق ـ إس سراً. فقد كان وضع الصناديق ـ إس في نظام معيار تشفير البيانات ينطوي على استبدلات وتغييرات أساسيَّة معقَّدة دونها أشد الأنظمة تعقيداً. وكانت أفضل طريقة يستطيع الغرباء التوسل بها لتقدير ما إذا كانت هذه التحولات الغريبة قد قصد بها إنتاج شيفرة أصعب من سابقاتها، أَو أنَّها خلعت سراً لتوضع في باب خلفي يتيح لوكالة الأَمن القومي تحقيق ميزة على سواها في تفكيك الشيفرات، يكمن في معرفة سبب اختيار المصممين معادلاتهم. وكان رفض الشركة شرح المنطق الذي يقوم عليه تصميم الصندوق ـ إس قد شجَّع نقاداً مثل ديڤي وهيلمان، على الاسترسال في شكوكهم والتفكير في مختلف النظريات التي تنطلق من فكرة الأبواب الخلفية السرِّيَّة.

وإن القول، بأن خوارزمية عامة معروفة للقاصي والداني، تأسَّست على مخطَّطات سرية أدَّى إِلىٰ شيوع حالة من الارتياب الشديد، وأصبح غذاء للنقاد استمر أعواماً. ولكن هذه الفكرة كانت بالنسبة للوكالة أمراً محسوماً، وغير قابل للنقاش. ولعل بنك العقول في فورت ميد رأى أنه قد يكون من قبيل الشر الذي لا بد منه، السماح بإطلاق خوارزمية شيفرة منيعة في عالم المصارف والشركات الضخمة. أما السماح بإذاعة التكنولوجيا المعقَّدة التي قد تشجّع الغرباء على اختبار شيفراتهم الخاصَّة. . . فأمر ما كانت الجماعة لتقبل به إطلاقاً.

كانت محصلة تلك الواقعة أنَّها اختزلت في ذاتها معضلة، على وكالة الأَمن القومي، أن تعترف بوجودها، ولو لنفسها. فقد ظل الجماعة في فورت ميد طوال سنين عديدة واثقين من أن مثل هذه المعلومات لن تخرج إلىٰ العلن، بعد ابتكارهم أسلوباً فذاً مثل تحليل الشّيفرة التفاضلي. ولكن تلك الأيام ولَّت. لنأخذ بعين الاعتبار أن مجموعة آي بي إم توصَّلت إلىٰ حالة الهجوم تي منفردة، دون معونة من الحكومة. وتحليل الشّيفرة التفاضلي هو في النهاية طريقة رياضية تنتظر الاكتشاف على يد كائن ما، خارج السياج الثلاثي، ولديه اهتمام بالشّيفرة المعقَّدة. وغني عن القول، أنَّه ما كان بوسع وكالة الأَمن القومي احتكار مثل تلك الحيل الرياضيَّة أكثر مما يستطيع عالم فلك اكتشف غمامة كونية لم يسبقه إليها عالم آخر، وكانت تغطي السماء ليتبينها راصد ذات يوم في المستقبل.

كانت هذه حقيقة العصر القادم: الشّيفرة العلنية: وسواء رضيت وكالة الأَمن القومي أم لم ترض، فإن أصحاب العقول الذكية لا بد وأن يكتشفوا من جديد الأفكار والأساليب التي كانت قيد الحجز في فورت ميد، ولعل هؤلاء سيأتون بعد، ببعض ما لم يكن ليخطر ببال حتى صفوة الكريبتوجرافيين وراء السياج الثلاثي.

إذا وضعنا الصناديق ـ إس جانباً، كان العنصر الأكثر مثاراً للجدل هو طول مفتاح معيار تشفير البيانات. كان لوسيفر الذي قدمه هورست فايشتل محدداً بمفتاح من 128 بت (خانة ثنائية)، لكن من الجلي أن وكالة الأَمن القومي ما كانت لترغب لمعيار التشفير القومي ـ وإن اقتصر استعماله على المؤسَّسات المالية والشركات الضخمة ـ أن يبقي المعلومات مقفلاً عليها في مثل هذه الخزانة الجبَّارة. ولذلك، ففي الوقت الذي شقت فيه الخوارزمية طريقها عبر السياج الثلاثي، وطرحت كمعيار قومي محتمل، تم اختصار طول المفتاح إلىٰ النصف، ثم زادوا في اختصاره حتى غدا هزيلاً نسبياً لا يزيد عن 56 بت.

وليس من العسير على المرء أن يتبيَّن أثر هذا الاختصار، فلنفترض أن أحد محلِّلي الشيفرة عجز، وهو يحاول اختراق معيار تشفير البيانات، عن اكتشاف طُرق مختصرة لتفكيكه. لذلك، فإن الطريقة الوحيدة أمام المتطفل لتفكيك رسالة مشفَّرة هي أن يشنّ هجوماً بالقوة الغاشمة، متوسلاً بكل تركيبة محتملة حتى يبلغ المفتاح الذي استخدم في عملية تشفير الرسالة الأصلية. وهذا البحث شبيه بحالة لص الخزائن الذي يجهد في تحريك قرص القفل حتى يعثر على مجموعة الأرقام التي تفتحه. وهو بحث يستحيل تنفيذه بالنسبة لمعيار التشفير، ولو استخدم المرء كومبيوتراً يستطيع إجراء الحسابات بسرعة عالية، وذلك بسبب «مدى المفتاح» الواسع جداً (المدى العددي الذي يحتوي كل تركيبات المفتاح الممكنة). والمفتاح الذي يتألَّف من 128 بت، هو مفتاح كبير جداً. وإذا حاول كومبيوتر التعامل مع مليون مفتاح كل ثانية ـ أي مليون مجموعة رقميَّة مختلفة على قرص الخزانة ـ لاستغرقت تجربة كل مفتاح محتمل، دهوراً.

ما هو تأثير اختصار المفتاح إلىٰ النصف؟ لتقدير هذا الأثر عليك أن تذكر طبيعة الحسابات الرقميَّة. إن كل بت (خانة ثنائية) في المفتاح الثنائي شبيه بشوكة على الطريق، لا بد لمفكِّك الشّيفرة من التعامل معها ليبلغ التركيبة الصحيحة من الوحدات والأصفار Ones and zéros. وكل شوكة تمثل اختياراً عشوائياً بين الدورة الصحيحة والدورة الخاطئة؛ والمفتاح الذي يتألَّف من 128 بت، يعني: أن عليك تقدير الطريقة الصحيحة لتحريك القفل 128 مرة في كل صف. ولمضاعفة صعوبة العملية، يكفي أن تضيف شوكة أخرى، وتكون بذلك قد ضاعفت عدد الطُرق المحتملة للتعامل مع الشيفرة مرَّتين. مع أن إحداها فقط هي الطريقة الصحيحة ما زالت على حالها. وبالمقابل، فلاختصار الصعوبة إلىٰ النصف، لا يتحتم أن تقسم عدد الشوكات إلىٰ النصف، بل يكفي أن تزيل شوكة واحدة وحسب.

ولذلك، فإن استبعاد بت واحدة من حجم المفتاح يعني أن الرسالة

المشفَّرة مأمونة بنسبة النصف عما كانت عليه من قبل. ثم إن الانتقال من مفتاح يتألَّف من 128 بت إلىٰ آخر يتألَّف من 127 بت، يعني اختصار عنصر العمل اللازم في حل الشّيفرة إلىٰ النصف. فإذا انتزعت منه بت أخرى، فأصبح حجم المفتاح 126 بت، تكون قد قسمته إلىٰ النصف. وهكذا دواليك.

ووفقاً لتكمان، فقد رأت مجموعة كينجستون أن مفتاحاً من 128 بت لا يعتبر إسرافاً فحسب، بل سوف يتطلَّب مساحة أكبر للرقاقة وحسابات أكثر أيضاً. وفي ذلك يقول: «لقد تحتم علينا وضع الخوارزمية كلها هناك، والصناديق ـ إس، وكل شيء. وكنا نستخدم رقاقات سي إم أَو إس CMOS [أنصاف نواقل تتمتَّع باستهلاك منخفض للاستطاعة. هـ. م.] بقوة 2 ميكرون، وكانت البيانات الواردة بعرض 8 بايت bytes [البايت يعادل 8 بت]. وهكذا كان طول المفتاح الأول 64 بت، وهي مناسبة تماماً لرقاقة واحدة، وعدد يقبل القسمة على بايتات مؤلفة من ثماني بتات.

كان هذا تقليصاً عظيماً، إذ اختزل الزمن اللازم للبحث الكامل على الكومبيوتر الذي يؤدي نظرياً عمله بواقع مليون مفتاح في الثانية، من بلايين السنين إلىٰ حوالي 300 ألف عام. ومع ذلك، فما زال طول المفتاح المؤلَّف من 64 بت كبيراً، في منتصف السبعينات، خاصة وأنّه كان من المتفق عليه أن تكنولوجيا الكومبيوتر ستظل دون التطور الذي يسمح بأعمال بحث بمثل هذا القدر، من السرعة على مدى العقدين التاليين.

لكن مجموعة كينجستون قامت، بعد ذلك، باختصار ثان، لم يكن في ظاهر الأمر مبرراً، بحيث أصبح طول المفتاح 56 بت، وهو من الناحية الرياضيَّة غير مناسب، وفجأة دخل الصورة احتمال الهجوم بالقوة الغاشمة. فما هي قيمة مجرد 8 بت حتى تحدث هذا التأثير؟ حسبك هنا التّذكّر أنّه كلما تقلَّص المفتاح بمقدار بت واحد، ازدادت سهولة تفكيكه بمقدار الضعف. وهكذا أدَّى اختزال الثماني بتات إلىٰ جعل حل الشّيفرة أسهل بمقدار 256 مرة، أي اختصار الزمن

من 300 ألف سنة إِلىٰ ما يزيد قليلاً عن ألف سنة. أَو بعبارة أخرى أن نسبة الصعوبة قد تقلَّصت، وأصبح بالإِمكان الآن استعراض مدى المفتاح في أقل من يوم واحد، بينما كان سابقاً قد يشغل كومبيوترات العدو ما بين كانون الثاني/ يناير وآب/ أغسطس.

فماذا كان تفسير آي بي إم لهٰذا الأمر؟ حسب قول تكمان أن الإجراء المتبع في الشركة في تصميم العتاد، كان ترك عدد معين من البتات الإضافية من أجل «تدقيق التكافؤ» Parity checks ضرب من التزامن للتأكّد من صحة قراءة الإِشارات الإِلكترونية. ويقول تكمان: «إنه من المواصفات الداخليَّة التي تحدّدها آي بي إم»، وهو يعترف في الوقت ذاته، بأنه شرط «أحمق» ويتابع قائلاً: «إننا لم نعد نأخذ به، لكن في ذلك الوقت كان لدينا معياراً، وهكذا اضطررت لتقليص حجم المفتاح [ليتسع للبتات الإضافية]».

لم يكن تكمان يعتقد أن في هذا التقليص الإِضافي، ما يعرض معيار تشفير البيانات للخطر فعلاً. (كان هورست فايشتل يعارض في قرارة نفسه هذا الرأي، ويؤثر مفتاحاً من 128 بت. غير أنَّه لم يعد مشتركاً في هذا المشروع، ثم سرعان ما ترك العمل في شركة آي بي إم ذاتها بعد حين). واعتقد تكمان وزميله كارل ماير بأن مفتاحاً يتألَّف من 56 بت بتنوعاته المختلفة، التي تبلغ 70 كدريليون، هو أكثر مما يلزم لحماية الأسرار التجارية، والمالية التي سيقوم بها معيار تشفير البيانات. ويذهب تكمان إِلىٰ أن الفكرة التي يقوم عليها المعيار هي توفير مستوى من الأمن لشبكات الكومبيوتر يماثل ما يتمتع به الناس في مجال عملهم الفعلي: «أدراج المكاتب المغلقة، للغرف التي تحتوي على الكومبيوتر، والمستخدمون الأوفياء ذوو اللباقة والكياسة». لم يكن المقصود حماية الأسرار العسكرية، التي تنقل عادة في حقائب يدوية منتفخة مربوطة إِلىٰ أيدي أشخاص يحملونها ويحرصون عليها، أَو يعهدون بها إِلىٰ جواسيس لديهم أوامر بابتلاع الحبوب السامَّة عند اعتقالهم.

وهناك آخرون، على كل حال، كانوا يعتقدون بأن هذا الاختصار مردّه ضغوط مارستها وكالة الأَمن القومي. ومن هؤلاء المرتابون داخل آي بي إم ذاتها، مثل ألان كونهايم، رئيس مجموعة الرياضيات في مشروع معيار تشفير البيانات. ويقول كونهايم معرضاً بوضوح عن التفسير الذي قدمه تكمان: «ست وخمسون بت أمر شاذ. [فلا بد] أن الحكومة قالت إن أربع وستين بت كبير جداً ـ فليكن 56 بت». فما الذي جعل الآي بي إم توافق على هذا الطلب؟ إنَّك تدرك أنَّ لها مصالح تجارية في جميع أرجاء العالم. ولا تستطيع تصدير قلم رصاص إِلىٰ خارج الولايات المتّحدة دون إجازة تصدير. وليس هذا كل ما في الأمر، فعندما تلوح [وكالة الأَمن القومي] بالوطنية والأمن القومي فإنك لا تملك المجادلة في هذه الأمور».

أما بالنسبة لغرباء أمثال: مارتين هيلمان وهويت ديفي، طبعاً، كان حجم المفتاح دليلاً على أن وكالة الأَمن القومي قد أضعفت مستوى المعيار خدمة لأغراضها المشبوهة. ففي الشهور التي أعقبت إشهار المعيار، دأب الكريبتوجرافيين في جامعة ستانفورد على توجيه سيل من الاقتراحات والاعتراضات إِلىٰ الجهة المكلفة بالاتصال في المكتب القومي للمعايير، وأخذ شعورهم بالإحباط يزداد، حين وجدوا المسؤولين هناك، لا ينقطعون عن القول بإلحاح على أنّه ليس في الموضوع ما يدعو للارتياب. ثم وصل هيلمان إِلىٰ القناعة بأن المكتب القومي للمعايير، لم يكن يمثّل رأي أعضائه، وإنما كان يؤدي دور العميل لفورت ميد.

وللبرهان على رأيه فيما يتصل بضعف حجم المفتاح، تحدى هيلمان مديراً تنفيذياً في شركة آي بي إم، كان يعرفه أن يدحض قناعته وديفي بأن مفتاح معيار التشفير هذا يمكن أن تتغلَّب عليه آلة قوية متطورة في يوم واحد. وفي ذلك الوقت، كان الباحثون في جامعة ستانفورد قد ذهبوا في تقديراتهم إِلىٰ أنه يمكن إنتاج آلة كهذه بكلفة 20 مليون دولار. وإذا أمكن معرفة مفتاح واحد كل

يوم، على مدى خمس سنوات، فإن كلفة تفكيك كل مفتاح 10 آلاف دولار. وهذا استثمار لا بأس به إذا تضمنت بعض الرسائل المفكَّكة بيانات هامة مثل مواقع مخزونات النفط الاستراتيجي، وخطط الدمج بين الشركات الضخمة ـ فمعلومات كهذه تعادل ملايين الدولارات. ويقول هيلمان: «وحتى لو بلغت الكلفة 100 ألف دولار فلن يضيرنا ذلك، لأن سرعة الكومبيوتر سوف تتضاعف عشر مرات خلال السنوات الخمس التالية، ولن يكلف الحل سوى عشر كلفته الحالية». ويروي هيلمان أن المدير المذكور في الآي بي إم وجَّه أمراً للباحثين لاستقصاء الموضوع، ويقول أن هذا المدير: «اتصل بي بعد حين وقال إن الأَرقام التي توصل إليها الباحثون لديه، تجري في الملعب ذاته مثلنا، كانت عبارة «في الملعب ذاته» هي العبارة ذاتها التي استخدمها [هذا المدير]. لكنه أفادني بأن حجم المفتاح حدَّده المكتب القومي للمعايير، وليس الآي بي إم».

وفي الوقت ذاته، كان المسؤولون في المكتب القومي للمعايير يؤكدون في ردودهم على رسائل هيلمان المتكرِّرة والتي كانت تزداد حدّة باطراد، أن دراساتهم تبين أن آلة كالتي يتصورها سوف تستغرق إحدى وتسعين عاماً لتستقصي مدى مفتاح معيار تشفير البيانات. وكان واضحاً أن هؤلاء القوم لا يلعبون في نفس الملعب الذي يلعب فيه هيلمان.

كان هيلمان يعتقد أن ذلك كله يعتبر دليلاً ساطعاً، على أن معيار التشفير كان منذ البداية خداعاً؛ فهو في الواقع، المخطط الأصلي، الذي وضعته وكالة الأَمن القومي. إن المكتب القومي للمعايير الذي يفترض فيه أنه غير خطر ـ هو الوجه العلني لوكالة الأَمن القومي ترك للآي بي إم تصميم الخوارزميات على نحو مستقل. وقد أتاح هذا الأمر [للمكتب القومي للمعايير ووكالة الأَمن القومي] إنكار كل علاقة لهما بالموضوع، فكان بالإِمكان عندئذ التملّص من أي التزام أَو ارتباط به، فإذا سئلوا، أجابوا: اسمعوا يا جماعة، لسنا نحن الأشباح من طبخ ذلك، وإنما صاحبة العلامة الزرقاء العتيدة (آي بي إم). لكن الأشباح،

إذ حملوا الشركة على اختزال حجم المفتاح إلىٰ مجرد 56 بت، وبات هزيلاً إلىٰ حد يثير الحنق، تحقّق لهم ما أرادوا ونالوا مبتغاهم. وفي هذا، يقول هيلمان شاكياً: «لقد كانوا يدركون أن السيطرة على حجم المفتاح من شأنهم، وبذلك، يستطيعون في نهاية المطاف السيطرة على قوة المعيار.

كان هذا التفسير هو الألطف فيما قيل. أما إذا شئت أن تنحو إلىٰ الشك والريبة ـ وكان هيلمان وزملاؤه ينحون إلىٰ الريبة بشدَّة، شأنهم في ذلك شأن أي مصمِّم شيفرة متمكِّن من موضوعه ـ فإنَّك سوف تظل تتساءل مع ذلك إن كان في الأمر باب سرِّي يتيح للمخادعين في فورت ميد تفكيك رسالة مشفَّرة ترسل عبر معيار تشفير البيانات خلال ثوان. وإلاَّ، فما الذي يحملهم على إحاطة مبادئ التصميم بالسرِّيَّة؟

وفي مطلق الأحوال، رفض هيلمان الأخذ بتقدير الحكومة بشأن الإحدى وتسعين سنة، وقرَّر تجاوز الموظفين في المكتب القومي للمعايير الذين كان يجري وإياهم مراسلاته. وفي 23 شباط/ فبراير 1976 بعث برسالة إلىٰ إليوت ريتشاردسون الذي كان بوصفه وزير التجارة، الرئيس الأعلى للمكتب القومي للمعايير وعرض له شكواه:

«إنني أكتب إليكم، والقلق الشديد يساورني، من أن تكون وكالة الأَمن القومي قد أثَّرت بطريقة خفية على المكتب القومي للمعايير بما يحد، بشكل خطير، من قيمة المعيار المقترح، ومما قد يشكِّل خطراً على خصوصية الفرد. إنني أعني بهذا القول معيار التشفير المقترح والذي قصد به أن يوفر الحماية للبيانات السرِّيَّة أَو الخاصَّة التي تستخدمها الهيئات الفيدرالية غير العسكرية. ولا ريب في أن هذا سيغدو معياراً مفروضاً بحكم الواقع في عالم التجارة أيضاً.

. . . إنني لعلى ثقة من أن وكالة الأَمن القومي وهي تؤدي دورها بمساعدة المكتب القومي للمعايير في التصميم والتقييم للمعايير الممكنة، قد ضمنت لنفسها القدرة على تفكيك شيفرة المعيار المقترح».

ولم يخفف الرد الذي تلقاه هيلمان من أرنست آمبلر، القائم بأعمال مدير المكتب القومي للمعايير، الكثير من الثورة التي كانت تجيش في نفسه. فبدلاً من الرد المباشر على الاتهامات التي وجّهها هيلمان، قدّم آمبلر بعض التعليقات العامة، دافع بها عن معيار التشفير، مطرياً وكالة الأَمن القومي لمساهماتها في ضبط الخوارزمية. ثم أرفق رسالته بأمر إداري يحدِّد «وظائف ومسؤوليات وكالة الأَمن القومي». وجاء هذا الأمر خلواً من الإشارة إِلىٰ العبث بخوارزميات القطاع الخاص.

في ذلك الصيف، انكبّ هيلمان وديڤي، وخمسة أكاديميين آخرين على معالجة ذلك النِّظام، وقدَّموا بحثاً بعنوان «نتائج محاولة أولية لتحليل شيفرة معيار تشفير البيانات التابع للمكتب القومي للمعايير». وكان هؤلاء الباحثون صريحين وواضحين في تبيان أسباب القلق الذي ينتابهم: إن كل خوارزمية حظيت بموافقة وكالة الأَمن القومي، كانت «عرضة للشكّ مسبقاً» لأن «الوكالة لا تريد نظاماً منيعاً فعلاً يفسد عليها عمليات تحليل الشّيفرة الاستخباراتية التي تنهض بها». ولذلك لم يكن مفاجئاً، أنَّهم وإن كانوا مقصّرين جداً عن تفكيك مفتاح معيار تشفير البيانات، فقد توصَّلوا إِلىٰ أنَّه لا يمكن الوثوق بهذا النظام. واكتشفوا، إِلىٰ جانب قوة المفتاح، ما اعتبروه «بنية مريبة» في الصناديق ـ إس، وربما كان هذا، كما ذكروا، «نتيجة... باب مفخّخ وضع عمداً.

أما رجل الآي بي إم والت تكمان، فقد رأى في شكاوى ديڤي وهيلمان مهزلة، منشؤها جنون العظمة والجهل معاً. فالرَّجل ليس عميلاً سرياً ـ بل كان معنياً بإنتاج سلعة ـ وقد قاد فريقاً بكل ما أوتي من القوة والكفاءة لإنتاج سلعة جيدة! وكان يوماً سعيداً حين أنجز فريقه أول جهازين من معيار تشفير البيانات. وكان هذان صندوقين من المعدن بحجم صندوق صباغ الأحذية، وكل منهما محشو بالرقاقات، ويقع بين الكومبيوتر الرئيس والموديم. وإن وجود مثل هذا الجهاز عند كل طرف ينقل البيانات، يسمح لجهازي كومبيوتر بالتخاطب عبر

مجرى سري منيع على المتنصتين، مهما يكن قول مارتي هيلمان. وقد أرسل أحد هذين الصندوقين إِلىٰ مقر شركة الآي بي إم في باريس، والثاني وُضع في مكتب ليو برانسكومب في إرمونك، وكان لهذين الصندوقين، بعد هذا، شأن في التاريخ. قام مكتب باريس بإرسال رسالة مشفَّرة إِلىٰ الآلة في أرمونك، التي قامت بعد ما تمت تغذيتها بالمفتاح المتماثل الذي يؤدي وظيفتي التشفير وتفكيك الشّيفرة معاً، بتفكيك شيفرة الرسالة وإعادتها إِلىٰ صيغتها الأصلية. ويذكر تكمان أن الرسالة أُرسلت بعد استقبالها، إِلىٰ طابعة صغيرة ونشرت في كافة الصحف التي تصدرها الآي بي إم. وكانت رسالة ليس فيها ما يضير، طبعاً، لأنَّه كان معروفاً للجميع أنَّها سوف تنشر على الملأ».

لكن هذه السعادة لم تكتمل، إذ نالت منها الهجمات التي شنَّها هيلمان وأصدقاؤه. واضطر تكمان وزميله كارل ماير إِلىٰ الدفاع عن نفسيهما في ورشتي عمل علنيتين، كان المكتب القومي للمعايير قد قام برعايتهما. وكانت ورشة العمل الثانية، التي عقدت في أيلول/ سبتمبر 1976، في مقر المكتب في جيتسبورج، في ولاية ماريلاند، الأحفل بالمنازعات والمشاكسات. وقد تمسَّك تكمان بموقفه وآرائه، قائلاً: «إني لم آت بخطأ!» وحجم المفتاح مناسب، وصنع آلة لتفكيكه لن يكلف هذا المبلغ المتدني المؤلَّف من سبع خانات الذي وصفه هيلمان بل 200 مليون دولار.

وإذا كان حجم المفتاح دون الطول المطلوب، فبوسع من يرغب، تصميم أجهزة لتشغيل معيار تشفير البيانات بضعف سرعته، بوساطة مفتاحين مختلفين. ولئن كانت هذه العملية صعبة التنفيذ، إِلاَّ أنَّها سوف تؤدي إِلىٰ زيادة حجم المفتاح حتى يبلغ 112 بت، وفي هذا ما يكفي لإرباك كل كومبيوتر لعين على سطح الكرة الأرضية طوال القرون القادمة. (ثم ظهرت بعد حين عملية عُرفت باسم «معيار تشفير البيانات الثلاثي» التي يستخدم فيها ثلاثة مفاتيح، وتتغلّب على أشد الهجمات تعقيداً وقوَّة. بيد أن هذا كله كان أمراً غير ذي شأن

من الناحية العملية، لأن نسخة المعيار التي حدَّدت بـ 56 بت، هي النسخة التي اقترحت للمعيار).

ولقد فشلت مناشدة تكمان في تهدئة النقَّاد. وكان هؤلاء يسألونه لماذا لا تنشر عناصر التصميم؟ هل وضعت في المعيار باباً مفخّخاً؟

ثم جاءت مشكلة الصحف. وقد تذمّر تكمان من أن «هؤلاء الأساتذة الجامعيين طرحوا الموضوع على صحيفتي النيويورك تايمز والواشنطن بوست. وبعد ذلك قام تكمان ذاته بإجراء مقابلة صحفية، بطلب من شركة الآي بي إم، حول هذا الموضوع. وبعد جولة قصيرة في صحيفة الواشنطن بوست وإلقاء نظرة على مكتبي الصحفيين: وودوارد وبيرنستين، اللذين أصبحا مؤخراً من المشاهير، كرر تكمان ما سبق أن قاله لمراسل صحيفة التايمز: «أن وكالة الأمن القومي لم تجر أي تعديل على الخوارزمية، ولا أقامت باباً سرياً. انتبهوا يا شباب، إن هذا ضرب من السخف؟ إننا لن نجازف بشركة الآي بي إم كلها، بوضع باب سرّي في آلة من صنعها».

ومع ذلك، فقد أخذت الدعاية مداها. وكان الوضع سيئاً في ذاته، بعدما أخذت صحف التايمز والواشنطن بوست والوول ستريت جورنال تنشر تصريحات تكمان والنقاد. بل الأسوأ من ذلك، أن والدة تكمان اتصلت به من معتكفها في فلوريدا بعد تقاعدها مبدية قلقها مما سمعت من الأصدقاء، بعد اطلاعهم على الصحف الصادرة في نيويورك، راجية ولدها الذي بدأ حياته على أروع ما يكون لطالب جامعي نبيه من بروكلين: «أرجوك، يا ولتر، أن تستقيل من الآي بي إم وتترك صحبة السوء هؤلاء». وأجابها تكمان مطمئناً بأنّه لن يدخل السجن ليجاور إيرليخان، وهالدرمان [عضوان بارزان في حلقة الرئيس السابق ريتشارد نيكسون، وقد حكم عليهما بالسجن لتورطهما في قضية ووترجيت] فهو رجل مستقيم.

بعد الدعاية جاءت جلسات الشهادة أمام لجنة الاستخبارات في مجلس الشيوخ. وكانت هذه الجلسات سرِّيَّة مغلقة، وتجري خلف الأبواب الموصدة، والتقرير النهائي لتلك الجلسات كان سرياً أيضاً؛ ولكن صدر ملخص عنه، ليطلع عليه الجمهور العريض. فقدمت محتوياته ذخيرة لكلا الجانبين.

فمن جهة، تبين أن هيلمان كان على حق في إصراره على ما هي السلطة، التي فرضت المفتاح بطول 56 بت: «أقنعت وكالة الأَمن القومي شركة آي بي إم بأن مفتاحاً مختزلاً من 56 بت واف بالغرض». حسب ما ورد في التقرير. ولم يكن السبب في هذا الاختزال، كما ادعى تكمان، صرامة تصميم الرقاقة أو الحاجة لتدقيق التكافؤ، بل ضيق الحكومة بما يزيد عن هذا المفتاح. وكانت الشركة تدرك أن تصدير الجهاز مشروط بترخيص من الحكومة بعد الموافقة على المستورد. ولكن وكالة الأَمن القومي، المكلفة بالتعاون مع المكتب القومي للمعايير في تقييم معيار تشفير البيانات، باعتباره معياراً حكومياً، ما كان متوقعاً منها قطعاً أن تمهر بخاتمها خوارزمية تستخدم، في رأي الوكالة، مفتاحاً أطول مما ينبغي. وهنا يبدو أن المفتاح ذو الـ 56 بت، قد وفَّر لوكالة الأَمن القومي قدراً من الارتياح. ولئن كان العمل المطلوب لتفكيك شيفرة بهذا القدر من الطول، كبيراً إِلىٰ حد الإجهاد، فمن الواضح أنَّه إذا كان ثمة من يريد القيام بهجوم بالقوة الغاشمة لتفكيك شيفرة المعيار (ديز)، فهذه الجهة هي وكالة الأَمن القومي ذاتها، بما لديها من أجهزة كومبيوتر ضخمة ذات قدرات هائلة، في الطابق الأرضي من مبنى القيادة ومحاطة بأقصى قدر من السرِّيَّة. وغني عن القول أن الشّيفرة المثالية بالنسبة لمستخدمي الجهاز هي أقوى الشيفرات الممكنة، بينما الشيفرة المثالية لوكالة الأَمن القومي، من الناحية العملية، هي الشيفرة التي تكون من القوة بما يحول دون اختراق المجرمين والخصوم الآخرين لها، ومن الضعف بما يسمح للمليارات من دورات الكومبيوتر الخفية التي تعمل في فورت ميد من تفكيكها. فهل كان المفتاح

بطول 56 بت، هو المفتاح الملائم الذي يلبي هذه الشروط؟ هذا ما لم تجب عليه الوكالة. بل ولن تجيب.

ولقد خلصت اللجنة، بالرغم من الاستنتاج الذي وصلت إليه من أن حجم المفتاح تحدد بطلب من الوكالة، إلىٰ أنه ليس في الأمر خلل في العمل، سواء من جانب شركة الآي بي إم أو من جانب الحكومة. وقد كان قرار اللجنة أن حجم مفتاح معيار تشفير البيانات قد تقرَّر بشكل معقول. وكان على مارتي هيلمان وأصحابه القبول به، أعجبهم ذلك، أم لم يعجبهم.

استغرق الأمر بضع سنوات، لكن الجماعة لم يسلموا به في نهاية المطاف وحسب، بل كان عليهم كذلك مواجهة بعض الحرج. فكما لاحظ والت تكمان بزهو لم يكن هناك طوال عقدين من الزمن بعد قبول الخوارزمية رسمياً معيارين في عام 1977 من استطاع أن يجد وسيلة مختصرة لتفكيك رسالة مشفَّرة بمعيار تشفير البيانات. (طبعاً إذا كانت وكالة الأَمن القومي قد تمكَّنت من ذلك، فإنَّها لن تصرِّح بذلك على الإطلاق).

في عام 1990 كشف محلِّلو الشيفرات خارج هذا النطاق عن أسلوب تحليل الشيفرة التفاضلي، وأثبتوا أن بوسع المرء، في ظروف معينة (وهي كما يسلمون، نادرة) معرفة مفتاح معيار التشفير، بقدر أمل من الحساب مما يقتضيه الهجوم بالقوة الغاشمة. لكن هذا كان بالضرورة «الهجوم آتي» الذي اكتشفته الشركة أثناء عملية التطوير التي قامت بها لتقوية الخوارزمية وتدعيمها مقابل هذا الهجوم. وقد ظلَّت الآي بي إم تبقي الأمر سراً امتثالاً لطلب وكالة الأَمن القومي. (وهناك جماعة من الباحثين، خرجوا لهجوم نظري آخر على المعيار، هو تحليل الشّيفرة الخطي، سنة 1993 ـ لكن لا هذه الجماعة ولا تلك، تمكَّنت من طرح تهديد للشيفرة).

وهكذا إذا كان حجم المفتاح هو نقطة الهجوم الوحيدة على معيار تشفير البيانات. وإذا كان لا بد للمرء من تكريس طاقات حسابيَّة ضخمة لتفكيك رسالة واحدة، ثم عليه أن ينتظر أياماً وأسابيع وشهوراً حتى تنهار الشّيفرة، فإن وكالة

الأَمن القومي تكون قد أجازت أداة خارقة القوة لنشر أسلوب تشفير منيع في كافة أرجاء البلاد، وربما العالم أيضاً. ولطالما حمل القوم وراء السياج الثلاثي الانطباع بأن مستخدمي معيار التشفير سيكونون من المؤسَّسات المحافظة الموثوقة مثل المصارف والبيوتات المالية. لكنَّهم أخطأوا التقدير. فبدلاً من ذلك، جاء تطوير معيار التشفير، إيذاناً ببداية عهد جديد لوسائل رخيصة الكلفة وفعَّالة في استخدام الكومبيوتر للحفاظ على خصوصية المعلومات الشخصية. فلم يقتصر استخدامه على المصارف وحسب، وإنما امتد ليشمل كافة الاتِّصالات التجارية، بل بات شائع الاستخدام في الاتِّصالات الخاصة أيضاً. ومع احتفاظ وكالة الأَمن القومي بالسيطرة على تصديره، فإنَّه سرعان ما انتشر في حدود الولايات المتّحدة دون عائق أَو قيد. ولئن ظل المصنعون يخضعون لقيود التصدير ولا يستطيعون تسويقه وراء البحار، فالخوارزمية ذاتها، وجدت طريقها لتتسرّب إِلىٰ الخارج، مما أتاح للمطورين الأجانب أن يخرجوا بنسخهم الخاصة عنها.

ولربما سر البعض في فرع أمن الاتِّصالات المسؤول في وكالة الأمن القومي عن حماية البيانات الأمريكية وهي تدور في أنحاء الكرة الأرضية، لحلول هذا العهد الجديد من الحماية. لكن هذا الأمر قد أثار نوبة ذعر بين العاملين في مجال استخبارات الإِشارة، أي الذين كانت مهمتهم أن يكفلوا لجماعتنا سرعة اعتراض وتداول المعلومات الدسمة التي تجري حول الكرة الأرضية بصورة نبضات إِلكترونية. فإذا جرى تشفير هذه النبضات، وغدت لا تقبل القراءة بسهولة، فسوف تقوم عندئذ مشكلة. ومما زاد في الأمر سوءاً، ظهور تقنيات كومبيوتر زهيدة الثمن، أتاحت ـ بل فرضت القاعدة ـ تغيير مستخدمي معيار التشفير للمفاتيح، ليس كل بضعة شهور، كما افترضت وكالة الأَمن القومي، وإنما بصورة يومية أَو أكثر من مرة كل يوم.

أجل، لقد كان معيار تشفير البيانات مشكلة تشغل الفورت ميد. وبعد

سنوات، بات حتى مارتين هيلمان، يدرك أن هجومه على المعيار كان يقوم على عنتريات أكثر مما يستند إِلىٰ أساس صلب، وعلى حد قوله: «كانوا [وكالة الأَمن القومي] يمثلون العملاق، وأنا العقل الجبَّار. كنت أناطح الوكالة وهذا أمر من شأنه أن يدير رأس من كان شاباً في مقتبل العمر». أما الآن، فهو يعترف بأن للقضية وجهين: هما أن معيار تشفير البيانات كان بالرغم من حجم مفتاحه قوياً بما يكفي لتوفير قدر من الأمن للناس، ثم إن العملية ذاتها أشد تعقيداً وتكلفة، من مجرد قراءة نص معترَض غير مشفر، وإن كان لوكالة الأَمن القومي القدرة على تعبئة المصادر المالية والتقنية والعلمية والبشرية، على ما يفترض لتليين مفتاح معيار التشفير وإخضاعه بالهجوم بالقوة الغاشمة. وكان معيار التشفير أول درس تلقته وكالة الأَمن القومي بأن عصراً جديداً من أمن الكومبيوتر قد أطل، والمؤكد أنَّه سوف يعقد لها الحياة إِلىٰ حد كبير، ولربما إِلىٰ حد ضعضعة المؤسَّسة برمتها.

ويذهب آلان كونهايم إِلىٰ الاعتقاد بأن القول الفصل في أمر معيار التشفير جاء من هوارد روزنبلوم، نائب الرئيس للبحوث والتطوير في وكالة الأَمن القومي، حيث تفكك الكومبيوتر الضخمة شيفرات أصدقاء البلاد والأعداء، وتمتحن الشيفرات التي قصد بها حماية أسرارنا الخاصة. ففي أحد الأيام، وبينما كان روزنبلوم وكونهايم يتحدثان عن معيار التشفير، أبدى المسؤول الكبير في الوكالة ملاحظة زلّ بها لسانه، لكن كونهايم بقي يتذكرها لسنوات طويلة، إذ قال: «لقد قمتم بعمل جيد أكثر مما ينبغي».

ويعلق كونهايم اليوم بسرور غامر: «ولم يكن المقصود بتلك العبارة حول الإطراء».

المفتاح العام

لئن كان هويت ديفي ومارتي هيلمان اعتبرا معيار تشفير البيانات عملية مشبوهة، وربما ضرباً من الاحتيال من جانب شركة آي بي إم وحكومة الولايات المتّحدة، فإن تقديمه كان بطريقة غريبة هدية هامة للباحثين في جامعة ستانفورد. ذلك أن ديفي وهيلمان بعد أن قاما بالبحث المستفيض في البيانات الفنية المتوفرة، المتعلقة بالمعيار المقترح ـ والنظر في ما أهمل طرحه علناً ـ باتا يمتلكان موشوراً جديداً يمكنهما من تقدير جهودهما في هذا المجال. فمنذ أن سمع ديفي أولى التقارير عن المعيار الحكومي ذات يوم من عام 1974، أثناء تناوله الطعام في لوي، المطعم الصيني الذي يرتاده عباقرة ستانفورد، أخذ يتساءل في سره عن احتمال قيام وكالة الأَمن القومي بوضع باب سري فيه. وقاده هذا التساؤل إِلىٰ سؤال أعمق، يتصل بمفهوم الأبواب السرية. فهل يمكن تصميم شيفرة بكاملها حول باب سري؟

إن تصميم مثل هذا النِّظام ينطوي على تحديات ضخمة، لأنه يفرض حل تناقض أساسي. فالباب السري يوفر لمن يمتلك المعرفة المناسبة، الوسيلة التي يتجاوز بها الإجراءات الأمنية ليصل سريعاً إِلىٰ الرسائل المشفرة، وهو أمر يبدو فعالاً. ولكن مجرد فكرة استخدام الباب السري في نظام أمني تبدو مجازفة

جنونية، وذلك لأن ثمة احتمالاً بأن يتمكن المتطفلون الأذكياء من إيجاد طريقة لاستغلاله. وهذه عين المشكلة التي ينطوي عليها الباب السحري في المباني: فإذا عجز الأعداء عن العثور عليه، كان بوسعك استخدامه للاختبار؛ أما إن استطاعوا معرفته فإنَّهم يتمكنون عندئذ من بلوغ المكان الذي تختبئ فيه.

وهذه المفارقة جعلت إمكانية تصميم مخطط لباب سري أمراً مثبطاً للعزائم. ذلك أن أقوى منظومات التشفير قد صمِّمت من كافة نواحيها، للحيلولة دون تسرّب محتوياتها. وإذن فالعبث في أجزائها الداخلية لتركيب باب خلفي ـ تسرب! ـ يمكن أن يؤدي بسهولة إلىٰ إحداث عدة نقاط ضعف دونما قصد. وعندما عرض ديفي هذا الأمر على هيلمان، توصل الرجلان كلاهما إلىٰ أن منظومة كهذه ستكون على الأرجح أمراً غير عملي. غير أن ديفي ظل يعتقد أن هذه المنظومة جديرة بالملاحظة، فأضافها إلىٰ قائمة كان يقوم آنذاك بإعدادها بعنوان «معضلات نظرية كريبتوجرافية طموحة».

ومع ذلك، ما زالت الأمور كما هي في بدايات عام 1975، والأسابيع تمضي بلا طائل، بالرغم من جهود ديفي السيزيفية [نسبة إلىٰ أسطورة سيزيف الإغريقية] والتعاون المثمر الذي كان قائماً بينه وبين هيلمان. فهل كان مآل هذا الجهد الذي يقوم به للإحاطة بالكريبتوجرافيا أن يضيع ويذهب هباء؟ لقد كان لهيلمان وظيفة، على الأقل، تشغله. أما ديفي فكان بدون عمل. ومع أن الفترة التي أمضاها في العناية ببيت جون مكارثي كانت على قدر من الإمتاع، إلاَّ أنه تجاوز اليوم الثلاثين من عمره ولا دخل لديه، ولا تأتيه أبحاثه إلاَّ ببعض الدريهمات، وكان واضحاً أنَّه لن يستطيع التغلّب على العقبات التي لا بد له من تجاوزها قبل أن يفوز بشهادة الدكتوراه. ومع أن ديفي كان مبتهجاً بطبيعته، إلاَّ أن هذه الأمور التي كان يفكر ويعيد التفكير فيها باستمرار كانت مثبطة للعزائم.

وتسترجع ماري فيشر، مناسبة بلغت فيها معنوياته أدنى درجاتها، حين

دخلت غرفة نوم آل مكارثي ذات يوم، فوجدت ديفي واضعاً رأسه بين يديه وهو يجهش بالبكاء. وتقول: «سألته عن سبب بكائه، فأجابني أنّه لن يكون له شأن في الحياة قط، وعليّ أن أبحث عن شخص آخر [أرتبط به]، وأنّه ـ وأنا أذكر عباراته بالضبط ـ باحث عجوز منهار [بلا مستقبل].

ولقد حاولت التخفيف عنه والتهدئة من روعه. وقالت له يومذاك أنه رجل عظيم، إِلاّ أن العالم لم يدرك، بعد، هذه الحقيقة. وكانت ماري تدرس المصريات، فأخذت تشرح له أن المصريين القدماء، كانوا يميّزون بين الخصائص الشخصية الأصلية والخصائص المكتسبة. وكانت تعتقد أن «العظمة» من الخصائص التي لا تكتسب، فهي من قوام الشخصية الأصلية، وحسب المرء أن ينظر فيراها متجلية في صاحبها. وقالت له عندئذ: «إنني أعلم ما أنا ناظرة إليه، وأعلم أنّك رجل عظيم».

ولم يكن ديفي يشعر بأنّه رجل عظيم، بل كان يشعر بأنّه رجل فاشل.

وفي أحد الأيام أحضر ديفي وهيلمان معهما عالماً يعمل في حقل الكومبيوتر في جامعة بيركلي، يدعى بيتر بلاتمان، ليشهد إحدى الحلقات الدراسيَّة غير الرسمية في موضوع الشّيفرة، والتي كانا قد دأبا على إقامتها في حرم الجامعة. وبعد انتهاء تلك الحلقة، أوصل ديفي بلاتمان بسيارته إِلىٰ مختبر الذكاء الاصطناعي في جامعة ستانفورد، وفي الطريق، أتى بلاتمان على ذكر صديق له يدعى رالف ميركل، وكان هذا منكباً على دراسة معضلة طريفة: كيف تستطيع أن تجري مكالمة مأمونة عبر خط غير مأمون، دون أن يكون بين الشخصين اللذين يتبادلان الحديث معرفة مسبقة؟ وغني عن القول أنّه طالما كانا على غير معرفة سابقة ببعضهما، فلن يكون هناك ما يسمح لهما بتبادل المفاتيح السرِّيَّة قبل أن يجري بينهما حديث خاص.

كانت هذه، بالنتيجة، صيغة مختلفة للسؤال الضخم الذي ظل يؤرق ديفي طوال سنوات، أي: هل من الممكن استخدام الكريبتوجرافيا لحماية شبكة

مترامية الأطراف من عدوان المتنصتين والراصدين الذين يعنيهم تسجيل ما يسري عبر الخطوط؟ (أو بعبارة أدق، كانت هذه الصيغة تعكس ملاحظة ماري حول المعضلة التي تشغل فكر ديفي: في عالم مليء بالناس غير الجديرين بالثقة، كيف يمكن للمرء أن يستمر في إقامة اتصال حميمي بشخص يثق به؟). ولما كان ديفي لم يحقّق نجاحاً يُذكر في التصدي للمشكلة، فقد قال لبلاتمان أن خطة صديقه مستحيلة التحقيق. ويعتقد ديفي أن لهجته العصبية قد حملت بلاتمان على الاقتناع برأيه. إلاّ أن ديفي، وإن كان يجادل عاطفياً باستحالة تحقيق مثل هذه الخطوة الضخمة، فقد كان يعتقد في سرّه بعكس هذا الرأي، وراح عقله يجري بسرعة لاستيعاب ذلك الذي عرضه صاحبه؛ وكأنما كان يشعر في أعماقه بضرورة وجود مثل هذا الحل.

كيف يمكنك أن تبتكر نظاماً يتيح لأناس لم يسبق لهم الالتقاء ببعضهم البعض أن يتحدَّثوا بحرية واطمئنان؟ وأين يمكن إجراء الأحاديث كلها بكفاءة التكنولوجيا المتقدمة على أن تكون محاطة بحماية الكريبتوجرافيا؟ وكيف لك أن تحصل على رسالة مبثوثة إِلكترونياً من شخص ما، وتكون على ثقة من أنَّها وردت من المرسل الذي تحمل الرسالة عنوانه؟

لقد جاهد ديفي أثناء بحثه لجمع المعلومات اللازمة في مناخ يكاد يكون كله سرياً. لكنه توصل إلىٰ حصيلة تفوق توقعات أي شخص: الدوال (التوابع) الوحيدة الاتجاه. الحماية باستخدام كلمة السر. التحقق من الصديق أو العدو. الأبواب السرية. كان عقل ديفي يوحي له بأن الحل للمشكلة السرِّيَّة، والخصوصية لا بد كامن في مكان ما بين هذه الحصيلة كلها. وكان يعلم أن التوفيق بين الحمايات المختلفة التي توفرها هذه الأنظمة أمر لا محيص عنه لبحثه. وفيما أخذ يقدح زناد الفكر، ويزداد انشغالاً بموضوعه، بدأ يدرك السبيل للإفادة من هذه التقنيات، في التحقق من هوية الطرف الآخر. فأخذ يصنطع في ذهنه وسيلة يمكنه بواسطتها تنفيذ مشروعه عبر التوابع الوحيدة

الاتجاه تلك الظاهرة الرياضية حيث لا يمكن عكس أمر بذات القدر من السهولة الذي جرى حسابه به. وإن خطة كهذه ستكون، كما كتب فيما بعد؛ «تحدياً لا يمكن أن يأتي الرد عليه إلاً من شخص واحد، إنما سيكون في نظر الكثيرين حلاً حقيقياً». إنه بعبارة أخرى، نظام من «التحقق من جانب واحد» يقوم على سوء الفهم المخالف الذي خرج به صديق بيل مان قبل عدة سنوات: باب سري يعتمد على الدالة (التابع) الوحيدة الاتجاه، حيث يمكن إجراء عكس العملية الحسابية التي يصعب إجراؤها، إن توفر للمرء بعض المعلومات عن أسلوب تنفيذ الحساب الأصلي.

ولقد أدّى هذا إلىٰ طرح موضوع المفتاح الذي سبق أن تناوله ديڤي في أحاديثه مع مكارثي حول التجارة الإِلكترونية. ولكن ذلك إنما كان نصف المعضلة. فما هو نصيب الخصوصية والسرِّيَّة من هذا؟ وهل يمكن أن تنجح فكرة الباب السري ذي الدالة (التابع) الوحيدة الاتجاه في نظام يحمل معضلتين: أولاً التحقق اللازم من كلمات السر المستخدمة في الكومبيوتر وسواها من أدوات التحقق والتثبيت، وثانياً سرية الاتِّصالات؟

في ذلك الربيع كان ديڤي قد استقر على نظام في الحياة اتبعه أثناء إقامته في بيت مكارثي. فكان يقوم بتحضير وجبة الفطور كل صباح لماري وسارة، ابنة مكارثي ذات الأربعة عشر عاماً. وإذا انتهى الفطور، مضت ماري إلىٰ عملها، بينما تذهب سارة إلىٰ المدرسة، فيما يبقى ديڤي في البيت. وفي صباح أحد الأيام من أيار/ مايو 1975، أمضى ساعات الصباح في التفكير وحيداً في البيت، بعد ذهاب زوجه وسارة. ثم عاد إلىٰ ما يشغل ذهنه بعد استراحة الغداء. وكان يفكر للمرة الألف بمشكلة وضع كلمة سر مأمونة في شبكة الكومبيوتر. وواجهته من جديد مشكلة توفر الإداري الموثوق الذي يحمل كلمة السر. فكيف تستطيع استبعاد ذلك الطرف الثالث من المشروع كلياً؟ وفي وقت ما بعد الظهر، وجد الأمور تنجلي له فجأة: ابتكار نظام لا يوفر كل ما كان

يتصوره ديفي مؤخراً من خطة للتحقق من طرف واحد وحسب، وإنما يستطيع أن يحقِّق التشفير وتفكيك الشيفرة بطريقة مبتكرة أيضاً. وهذه سوف تحقق له حل مشكلة الإداري غير الموثوق، والأكثر من ذلك كلياً.

كان الحل في تقسيمه المفتاح.

كان الاكتشاف الذي خرج به ديفي ينطوي على ما يبدو في تاريخ الكريبتوجرافيا هرطقة خالصة: مفتاح عام/ علني. حتى هذه النقطة كانت هناك، على ما يبدو، مجموعة من القوانين المندسة في التشفير، والتي تبلغ حدّ الفقيدة المسلَّم بها، ولا يملك أحد تجاوزها وإِلاًّ كان مصيره جحيم الكريبتو. ومنها أن المفتاح الذي جرى به «تشفير» الرسالة هو ذاته الأداة التي تُستخدم في فكّ تشفيرها. ولهذا السبب كان يشار إِلىٰ المفاتيح بالمتماثلة، ولهذا السبب أيضاً، كان الإبقاء على تلك المفاتيح سراً أمراً عسيراً جداً: لأن الأدوات التي يسعى إليها المتنصّتون، أي مفاتيح فكّ التشفير ذاتها، يجب أن تنتقل من شخص إِلىٰ آخر، وبالتالي تتواجد في مكانين، فتزداد بذلك احتمالات الخطر. ولكن ديفي الذي امتلأ دماغه بكمّ هائل من المعلومات التي تكبّد أشد العناء في جمعها، على امتداد نصف عقد من الزَّمن، بات يرى الآن احتمالاً، بوجود أسلوب آخر لمعالجة الموضوع. فبدلاً من استخدام مفتاح سري مفرد واحد، تستطيع أن تستخدم زوجاً من المفاتيح. ومؤدى ذلك أن المفتاح المتماثل، يُستعاض عنه بمفتاحين ديناميكيين، أحدهما يقوم بتشفير نص الرسالة، يؤدي مهمته على نحو يحول دون قراءتها من الغرباء، إنما مع تضمين الرسالة باباً سرياً. أما ثانيهما فهو أشبه بالقفل، ووظيفته فتح الباب السري ليسمح لحامله بقراءة الرسالة. وهاكم الروعة في هذه الخطة: أجل، إنه المفتاح الثاني ـ أي مفتاح الباب السري ـ وهو الجزء الثمين من هذا الترتيب الذي لا بدّ من إخفائه، طبعاً، وراء ستارة، بعيداً عن متناول المتنصتين المحتملين. أما القرين، المفتاح الآخر الذي يقوم بالتشفير، فليس من الضروري أن يكون سرّاً على الإطلاق.

بل الحق أنَّك قد لا ترغب في أن يكون سراً أصلاً، بل سوف يكون من دواعي غبطتك إشاعته بين القاصي والداني.

والآن، كانت فكرة توفير السرِّيَّة والخصوصيَّة باستخدام مفاتيح يجري تبادلها علناً، فكرة مجافية للبداهة، بل غريبة في ظاهر الأمر. ولكنها قد تنجح باستخدام رياضيات الدوال (التوابع) الوحيدة الاتجاه. وكان ديڤي يعلم هذا، وأدرك في لحظة إلهام أنه يستطيع تنفيذ الفكرة باستخدام تلك التوابع.

كان ذلكم هو الحل للمعضلة. ومنذ تلك اللحظة، أصبح كل ما في عالم الكريبتوجرافيا في حال غير ما كان عليه.

أولاً، أن ديڤي بتقديمه بديلاً للنُّظم التي تقوم على مفتاح متماثل واحد، أتى بحل لمشكلة كانت وثيقة الارتباط بنُظم الكريبتوجرافيا إِلىٰ حدّ أنَّه لم يكن ليخطر ببال أحد تقريباً، أن هذه المشكلة قابلة للحل: عنينا بذلك صعوبة توزيع هذه المفاتيح السرِّيَّة على من يتلقون الرسائل السرِّيَّة مستقبلاً. فإذا كنت تنظيماً عسكرياً فقد يكون بوسعك حماية مراكز توزيع المفاتيح المتماثلة السرِّيَّة (والله تعالى يعلم أنَّه في أشد العمليات حساسيَّة ثمة سقطات أو ثغرات). أما إذا انتقلت مثل هذه المراكز إِلىٰ القطاع الخاص، وجماهير الناس التي تضطر لاستخدامها، فلن يكون أمامك أكوام الأوراق من الإجراءات البيروقراطية الحتمية وحسب، وإنما التهديد القائم بالخطر من شيوع السرّ أيضاً. فانظر إِلىٰ الأمر إن شئت من الناحية التالية: إذا كنت مضطراً لتفكيك رسالة مشفَّرة، أفلا يكون وجود مكان يختزن جميع المفاتيح السرِّيَّة فرصة لشخص بغيض للحصول على هذه المفاتيح إن بالسرقة، وأو بالرشوة، أَو أي شكل من أشكال القسر؟

أما بوجود نظام المفتاح العام، فإنَّه سيكون بوسع كل شخص صوغ مفتاحه المزدوج الفريد، المؤلَّف من مفتاح عام وآخر خاص، ولا يمكن لطرف خارجي الوصول إِلىٰ الأجزاء السرية من المفتاح. وعندئذ يمكن للاتِّصالات الخاصَّة أن تجري.

وهاكم كيف يعمل المفتاح المزدوج: افترض أن أليس ترغب في الاتّصال ببوب. فإذا أخذنا بتصوّر ديفي، فإنَّها لا تحتاج إلاَّ إلىٰ المفتاح العام الذي يملكه بوب. وهي تستطيع حيازته بأن تطلبه من بوب، أو لعلّها تلجأ إلىٰ ما يشبه دليل الهاتف الذي يحتوي على المفاتيح العامَّة. لكن يجب أن يكون مفتاح بوب العام ذاته، مفتاحه الشخصي، وهو شريط طويل من البتات من وضع شخص واحد، ولا أحد سواه في العالم... بوب. ثم تقوم باستخدام ذلك المفتاح العام، بطريقة الدالة (التابع) الوحيدة الاتجاه، لتشفير الرسالة بحيث لا يمكن فكّ تشفيرها حسابياً إلاَّ بوساطة المفتاح الخاص. النص الآخر من ذلك الزوج الفريد من المفاتيح (وهكذا فالمفتاح السرّي هو «الباب السحري» في الدالة الوحيدة الاتجاه للباب السري التي كانت تشغل تفكير ديفي).

ولذلك حين تبعث أليس برسالتها المشفَّرة، فلن يكون هناك إلاَّ شخص واحد في العالم يملك المعلومات اللازمة لقلب المعادلة وتفكيك الشّيفرة: أي بوب حامل المفتاح الخاص. والآن لنفترض أن الرسالة المشفَّرة وقعت في يد شخص متلهف لمعرفة ما الذي قالته أليس لبوب، ومن يهتم بذلك؟ إذا لم يستطع المتطفل الحصول على الشريك الوحيد للمفتاح العام الذي يحمله بوب ـ الأداة التي استخدمتها أليس، لتحويل الرسالة إلىٰ ما هو أشبه بفوضى لغوية ـ فإن اعتراض الرسالة، لن يأتي للمتطفل بأكثر من تلك الفوضى. وبدون ذلك المفتاح الخاص، فإن عكس عملية التشفير رياضياً تغدو أمراً بالغ الصعوبة. تذكر أن السير في الطريق الخاطئ في الدالة (التابع) الوحيدة الاتجاه أشبه بمحاولة جمع قطع طبق العشاء إلىٰ بعضها البعض بعد أن غدت فتاتاً.

أما بوب فلا يجد، طبعاً، أي صعوبة في قراءة الرسالة الموجهة إليه حصراً. فهو يملك الجزء السري من المفتاحين، ويستطيع استخدام المفتاح الخاص في فك شيفرة الرسالة في لحظات.

وباختصار، فإن بوب يستطيع أن يقرأ الرسالة لأنه الوحيد الذي يملك كلا الجانبين من المفتاح المزدوج. أما الذين يملكون المفتاح العام، فلا ميزة لهم عندما يحاولون تفكيك الرسالة. أما حين يتصل الأمر بتشفير الرسائل، فإن القيمة الوحيدة لامتلاك مفتاح بوب العام يتجلّى، في النتيجة، بقلب الرسالة إلىٰ كلام بوب، أي اللغة الوحيدة التي يستطيع بوب وحده قراءتها (بفضل امتلاكه النصف السري من المفتاح المزدوج).

إن وظيفة التشفير هذه، إنما كانت جزءاً وحسب من التصور الثوري الذي أتى به ديفي، وليس بالجانب الأهم بالضرورة. فقد قدم المفتاح العام في الشّيفرة أول وسيلة فعّالة للتحقّق على الوجه الصحيح من هوية مرسل الرسالة الإِلكترونية. وإن الباب السري، كما تصوره ديفي، يعمل باتجاهين. فإذا قام أحدهم بإرسال رسالة مشفَّرة بوساطة مفتاح عام يخص شخصاً ما، فإن المرسَل إليه المقصود وحده الذي يستطيع قراءتها. أما إذا عكست العملية. أي إذا قام أحدهم بتشفير نص ما بمفتاحه الخاص، فلا يمكن فكّ التشفير إِلاَّ باستخدام المفتاح العام الذي يطابق قرينه المفتاح الخاص. ولعلك تتساءل عن الغرض من ذلك؟ إذا تلقيت رسالة من شخص يزعم أنه ألبرت آينشتاين، وتساءلت إن كان هو ألبرت آينشتاين حقاً، فإن لديك الآن طريقة للتحقق من صحة هذا الزعم، اختبار رياضي بمثابة الاختبار بمادة غبار الشمس الزرقاء. وذلك بأن تأخذ المفتاح العام لألبرت آينشتاين، ثم تطبقه على النص المشفّر. فإذا كانت النتيجة نصاً واضحاً ولم تخالطه الترهات، غدوت على يقين من أن آينشتاين هو صاحب الرسالة، لأنه يحمل المفتاح الخاص الوحيد في العالم الذي يمكن أن يقدم رسالة يستطيع مفتاحه العام الملازم للخاص أن فكّ تشفيرها.

ومؤدى ذلك بعبارة أخرى، أن استخدام المرء مفتاحه السري في رسالة ما، يعادل توقيعك: إنه توقيع رقمي digital signature. لكنه يختلف عن التواقيع

التي تظهر بها شيكات المصارف، وأوراق الطلاق، أَو تمهر بها كرات الرياضيين، فالتوقيع الرقمي لجون هانكوك، لا يمكن تزويره من أي شخص لديه قدر أدنى من المهارة اللازمة لتقليد خطوط صاحب التوقيع الأصلي وسماته المميزة. فالأمل ضئيل بأن يتمكن اللص منتحل التوقيع، من تقديم توقيع مزوّر بدون المفتاح السري.

كذلك ليس للمزور المحتمل، أمل برصد خط هاتف شخص ما، ثم الإنتظار حتى يظهر التوقيع الرقمي لضحيته، فيلتقطه بغرض استخدامه في تزوير الوثائق أَو اعتراض الرسائل مستقبلاً. ذلك أن التوقيع الرقمي لا يلحق عملياً بالوثيقة أَو الرسالة. بل يتداخل بصورة وثيقة مع الأرقام التي تشكّل محتوى المادة المرسلة كلها. فإذا ما تم اعتراض الرسالة، فإن المتنصت لن يتمكّن أن يستخلص منها الأدوات اللازمة ليضع توقيع المرسل على وثيقة أخرى.

إن هذا الأسلوب يكفل، صحة الوثيقة برمتها. فليس للعدو أملٌ بتغيير جزء صغير من الرسالة الموقعة رقمياً، إنما سيكون التغيير كبيراً (مثل تبديل النص من «إني لست مسؤولاً عن ديون زوجتي» إلىٰ «إني مسؤول عن ديون زوجتي» وتوقيع المرسل الغافل محمول بالرسالة). وإذا كانت الرسالة موقعة رقمياً بمفتاح خاص، إنما دون تشفير، فبوسع ذي القصد المريب أن يعترضها ويستخدم المفتاح العام للمرسل الموزع على نطاق واسع لتفكيك الرسالة، ثم يعمد بعدئذ إلىٰ إحداث التغيير في النص غير المشفّر. ولكن ماذا بعد هذا؟ إن صاحبنا المزوّر سوف يحتاج، لكي يعيد إرسال الرسالة من جديد إلىٰ المفتاح الخاص لمهر الوثيقة بكاملها بالتوقيع. سوى أن هذا المفتاح لن يكون متيسراً، لأنه يبقى دائماً في حوزة المرسل الأصلي.

كذلك من الميسور للمرء أن يبعث برسالة محاطة بالسرِّيَّة فضلاً عن مهرها بالتوقيع. فإذا أراد مارك مثلاً أن يوجِّه أمراً إِلىٰ مديرة المصرف الذي

يتعامل معه، لينور، فإن أول ما يفعله هو توقيع الطلب بمفتاحه الخاص، ثم يقوم بتشفير الرسالة باستخدام مفتاح لينور العام. فتتلقى لينور رسالة مشفَّرة مرتين: مرة ابتغاء السرِّيَّة، ومرة للتثبت والتحقّق. فتستخدم أولاً مفتاحها السري لفتح مغاليق الرسالة التي لا تستطيع سوى عينيها قراءتها. ثم تعمد إِلىٰ استخدام مفتاح مارك العام، لتفك الرسالة التي تعلم أن صاحبها لا يمكن أن يكون سوى مارك.

وللتوقيع الرقمي، ميزة أخرى تتجلّى في استحالة إنكار صاحبه لدوره في توجيه الرسالة، لأنه لا يمكن لشخص سواه أن يأتي بمثلها وهي الموقعة رقمياً، وهو ذاته الذي يحمل المفتاح الخاص الذي قام بعملية التشفير. وهذه الميزة الملزمة بقبول نص الرسالة تعادل خاتم الكاتب العدل.

ولقد أصبح من الممكن لأول مرة إجراء كافة المعاملات الرسمية من عقود وإيصالات وما شابه بوساطة الكومبيوتر دونما حاجة لمثول صاحب العلاقة شخصياً للتنفيذ.

باختصار، لم يأت ديفي بطريقة تكفل السرِّيَّة والخصوصية في عصر شاعت فيه الاتصالات الرقمية وحسب، بل فتح الطريق كذلك إِلىٰ قيام شكل جديد كلياً من التجارة، هي التجارة الإِلكترونية التي لديها القدرة، لا أن تضارع الوثائق المعتمدة في التجارة حالياً فقط، وإنما أن تتفوَّق عليها أيضاً. والأدعى للإعجاب، أن إنجازه كله تم بعيداً عن رقابة الوكالات الحكومية التي تمتلك حتى أصغر التفاصيل، لأكثر أنظمة الكريبتوجرافيا غموضاً.

ويا له من نصر لهويت ديفي! ثم يا له من ذعر أصابه حين كاد، في لحظات، بعدما تفتق ذهنه عن أهم كشف في تاريخ الكريبتوجرافيا، أن ينسى ذلك كله. كان قد نزل إِلىٰ الطابق الأرضي ليتناول زجاجة من المياه الغازية، وفي لحظة رهيبة واحدة وجد أن كل ما خطر بباله قد تسرَّب وتلاشى. فدار حول منضدة المطبخ، وإذا به يستعيد خواطره كلها، هكذا بسرعة البرق. إِلاَّ أن

تلك الأفكار باتت لصيقة في هذه المرة لا تغادر رأسه. ومع ذلك، فإنه لم يعمد إلىٰ تدوين أفكاره، ثم لمع في خاطره، فجأة، أن الكومبيوتر الذي كان يحفظ فيه ملاحظاته غير آمن. ولم يكن بالمستطاع حينذاك أن يقوم بتشفير أفكاره منعاً لوقوعها في يد المتطفلين. وإذن، فلا محيص له من أن يطلع مارتي هيلمان عليها وجهاً لوجه، حين يلتقيه.

لكن كان عليه أولاً أن ينتظر عودة ماري إلىٰ البيت من عملها.

حينما عادت ماري فيشر من عملها في شركة بريتش بتروليوم، وجدت زوجها ينتظرها عند الباب، وكان ذلك من غير عادته. وقد ارتسمت على وجهه نظرة غريبة، وسمعته يدعوها إليه إذ لديه ما يحدّثها به.

قال هويت ديفي: «أعتقد أنني حقَّقت اكتشافاً عظيماً».

وراح يشرح لها فكرته. ومع أن جانب الرياضيات من الموضوع يتجاوز إمكاناتها، إلاّ أن التصور الذي عرضه كان مفهوماً لديها بشكل صحيح. والأكثر من ذلك أن ماري التي لاحظت زوجها طوال سنوات عن كثب، وهو يصارع المشكلة، وجدت الحل مناسباً بل شعرياً كذلك. وتقول ماري في زوجها المولود تحت برج الجوزاء: «لطالما كان ذا شخصية مزدوجة، وأحسب أن فكرة تقسيم المفتاح نشأت من ذلك التوتر».

بعدما حقَّق هذا كله لم يعد باحثاً عجوزاً منهاراً.

في تلك الليلة، نزل ديفي مشياً على الأقدام من التل إلىٰ منزل هيلمان ليحدثه، لأول مرة، في أمر المفتاح العام. ولقد استغرق الأمر بعض الشرح، إلاّ أن هيلمان سرعان ما أدرك أهمية ما تمخض عنه العصف الدماغي لديفي. لكن بقي على الاثنين أن يصوغا هذا في مقال علمي، ثم ينشراه. وكان مارتي هيلمان يعرف المكان المناسب؛ فقد تلقى دعوة قبل حين لكتابة دراسة حول التفاعل المتبادل في نظرية المعلومات لمجلة آي إي إي إي IEEE، فانتهز

المناسبة، وعرض على رئيس تحرير المجلة اقتراحه بأن يتعاون وديفي في تطوير هذا التصور، فرحّب بالفكرة أشد الترحيب (IEEE هي الأحرف الأولى لـ Institute of Electrical and Electronical Engineers مؤسَّسة مهندسي الكهرباء والإلكترونيات، وهي جمعية أكاديمية هندسية مرموقة، وتتولّى إصدار عدد من المجلات، ولبعضها أشد النفوذ في مجالاتها). فشرع الاثنان في العمل فوراً، وهما يواجهان حقيقة أن كل ما لديهما هو هذا التصور الذي اكتشفه ديفي وما ينطوي عليه من إمكانية الانتقال بالكريبتوجرافيا إلىٰ عصر جديد.

كان هذا التصور يبدو أحياناً، حتى لهيلمان، كما يتذكر فيما بعد، «ضرباً من الجنون». وفي أحد الأيام قرّر اطلاع زميله القديم في شركة آي بي إم، هورست فايشتل. وكان ما جرى بينهما حديث غريب. ذلك أنَّه ما أن شرع هيلمان في الكلام حتى قال له فايشتل أن لديه عشرين دقيقة فقط للحديث، لأنه في طريقه إلىٰ موعد مع الطبيب. فأخذ هيلمان يعرض له بسرعة أنه وديفي قد تغلبا على مشكلة توزيع المفتاح بوساطة باب سرّي يعتمد على الدالة/ التابع الوحيدة الاتجاه، ويسمح لك باستخدام مفتاح عام/ علني؛ لكن فايشتل لم يقبل بذلك على الإطلاق. وقرّع هيلمان قائلاً: «إنَّك لا تستطيع تنفيذ هذا الذي تقوله!» وتابع يحاضر فيه من أن الكريبتوجرافي الفلمنكي العظيم أوجست ليرتشوف قد وضع في كتابه العظيم: الكريبتوجرافيا العسكرية La Cryptographie Militaire، الصادر عام 1881، ست قواعد صارمة ينبغي ألا يحيد المرء عنها عند وضع شيفرة مأمونة، وإحداها: أن السرِّيَّة كلها ينبغي ألا تكون في النِّظام، بل في المفاتيح. وخلص عبقري الآي بي إم الذي كان وراء جهاز لوسيفر إلىٰ التساؤل، كيف لكما حتى أن تفكرا بجعل المفتاح عاماً وعلنياً؟ (لو لم يكن فايشتل علىٰ عجلة من أمره لمقابلة الطبيب، فربما كان قد أدرك أن فكرة ديفي وهيلمان، تتمثّل بكثير من الكياسة للشروط الصارمة التي وضعها كيرتشوف، من حيث أن أمن نظام المفتاح العام يكمن في حقيقة أن المفتاح الخاص يظل أبداً في ملك صاحبه ولا يستطيع الوصول إليه أحد سواه).

إِلاَّ أن فايشتل كان على صواب في أمر واحد، وهو أن التصور الذي أتى به ديفي هرطقة. لكن «الهرطقة هي طريق التغيير» على حد قول هيلمان. ولقد انقطع هذا الثنائي طوال الأسابيع القليلة التالية للعمل المحموم على بناء الأساس الرياضي لنظرية المفتاح العام في الكريبتوجرافيا. وكان هيلمان قد عرف في تلك الأثناء السبيل إِلىٰ نجاح تعاونه مع صديقه الزئبقي: «غالباً ما كان هويت يرى، وهو يقلب أفكاره، أمراً ما في شكله الجنيني، أولاً، فالتقطه أنا، لأجعل منه نتيجة أكثر صقلاً».

وفي هذه الحالة كانت النتيجة بحثاً بعنوان: «أساليب كريبتوجرافية لعدة مستخدمين». كان هذا البحث، بمعنى ما، عملاً مرجعياً يعبِّر عن فكرة المفتاح العام، بينما كان صاحباه يحرقان خلايا عقليهما وهما يحاولان العثور على طريقة، لتنفيذ هذا التصور وتطبيقه فعلاً. وقد اعترفا في بحثهما المنشور بأن: «ليس لدينا الآن لا البرهان على وجود أنظمة تقوم على المفتاح العام ولا نظام للعرض العملي». ومع أنَّهما كانا قد أرسيا الأساس الرياضي لمثل هذا النِّظام، فقد ظلا يتابعان البحث في الظلام عن التوابع الدقيقة ـ وخاصية الدوال (التوابع) الوحيدة الاتجاه للباب السري ـ التي تكفل تحقيق هذا التصور. ومع ذلك، فإن أولئك الذين تلقوا المسودات الأولى للبحث، وجدوا فيه انعطافاً مثيراً للدهشة، عن الحكمة التقليدية السائدة في الكريبتوجرافيا، وإغارة على أرض لم يجرؤ أحد، منذ عهد تريثيميوس حتى تورينج، على الخوض فيها.

أحقاً كان ذلك؟ طبعاً لو أن أحداً من وراء السياج الثلاثي أَو أياً من أبناء العم الأجانب قد خرج بهذه الفكرة لما علم بها هيلمان وديفي. ولو أن أحداً من العلماء نشر فعلاً بحثاً في هذا الموضوع، لكان ديفي قد وقع عليه، بالتأكيد، أثناء البحث الواسع الذي اضطلع به في السنوات القليلة الماضية.

ولقد تبين أن ثمة شخصاً واحداً على الأقل، تشغل فكره ذات الأفكار التي كانت تشغل ديفي وهيلمان.

في أوائل شباط/ فبراير 1976 تلقَّى مارتي هيلمان رسالة غريبة من طالب يحضّر لنيل شهادة الدكتوراه من جامعة كاليفورنيا في بيركلي:

> عزيزي الدكتور هيلمان
>
> قبل ثلاثة أيام حصلت على نسخة من ورقة عمل لك بعنوان «أساليب كريبتوجرافية لعدة مستخدمين». وكنت قبيل اطلاعي على هذا البحث قد انتهيت من تنقيح بحث [لي] في الموضوع ذاته، ولسوف يقدم قريباً في كوميونيكيشنز أوف ذي أيه سي إم Communications of the ACM [جمعية الآلات الحاسبة Association of Computing Machinary]. (جرى تقديم البحث أصلاً في آب/ أغسطس 1975). وقد أرفقت بهذه الرسالة نسخة من هذا البحث آملاً أن تجد فيه ما يثير اهتمامك. والحق أني مسرور إذا علمت أن هناك شخصاً آخر معني بهذه المعضلة. فالذين أحاول مناقشتها وإياهم إما عاجزون عن فهم مجريات الأمور، وإما يعتبرون الحل أمراً مستحيلاً. ولحسن الحظ، أن الحل (الجزئي) المعروض في البحث المرفق أثبت أنَّه ممكن. والآن، لو أننا نستطيع أن نتجاوز ما بلغناه! . . .

وانتهت الرسالة باقتراح: «إن إمكانية القيام بعمل مشترك مطروحة، وإنني معني بهذا الاحتمال. وأرجو أن يبلغني منك رد، متمنياً لك التوفيق في مسعاك».

وكان التوقيع باسم رالف ج ميركل، وعنوانه، في بيركلي يعكس كما يبدو، على سبيل المصادفة، السرعة التي باتت تسير بها الأمور هيست ستريت Haste Street (Haste تعني عجلة).

وفي الواقع أن اسم ميركل كان قد ظهر قبل بضعة شهور من ذلك

التاريخ: إذ كان هذا الطالب في بيركلي سبق أن ذكره لديڤي صديق مشترك، هو بيتر بلاتمان، وهذا ما حفز ديڤي على تشغيل آليات التفكير عنده وإقامة رابطة المفتاح العام الحاسمة. وقد بدا الآن أن ميركل قد أحدث انطلاقة، شبيهة بانطلاقة ديڤي، معتمداً في أبحاثه على جهوده المستقلّة، ولا عدة لديه سوى دماغه. وفوق ذلك أنَّه حسب ما ورد في البحث غير المنشور الذي أرفقه برسالته، قد نفذ الحيلة التي كان هيلمان وديڤي ما يزالان يتعثَّران في تحقيقها، إذ وضع مخططاً لمفتاح خاص.

كان ميركل ابناً لرجل مثقف، شأنه في ذلك شأن مارتي هيلمان وهويت ديڤي؛ فوالده كان المدير المساعِد لمخبر لونرس ليفرمور، وهو أحد أبرز مؤسَّسات البحوث العسكرية في البلاد، حتَّى توفي بسرطان القولون عام 1966. (تمتد مآثر آل ميركل إِلىٰ عم أبيه، فرد، وكان لاعب بيسبول، وعرف بهفوة شهيرة، هي إهمال لمس اللاعب الثاني، أثناء مباراة حاسمة لتحديد الفائز في راية السباق الوطني للأندية عام 1908). وكان الفتى رالف ميركل، كما هو مفهوم، هاوي علم ومبرزاً في الرياضيَّات، ولما انتسب إِلىٰ الجامعة في بيركلي، بات متحمساً للكومبيوتر. أما بالنسبة للكريبتوجرافيا، فيخبرنا أنه «لم يبد أي اهتمام كبير ملحوظ في هذا الحقل». ولكن الحال تبدّل في فصل الخريف الجامعي عام 1974، حين اختار في الفصل الأخير، قبل التخرّج، دراسة مشروع دراسي يعرف بـ «سي إس 244» CS 244 في موضوع سلامة وأمن الكومبيوتر. قام بتدريسها لانس هوفمان، وهو أستاذ مساعد في قسم الهندسة الكهربائية وعلوم الكومبيوتر. وكانت الشروط الأساسية للنجاح في هذه الدورة تنفيذ مشروع، بالإِضافة إِلىٰ تقديم امتحان في شهر تشرين الثاني/ نوفمبر. وحسب قول هوفمان «إن علامات النجاح متدرجة بشكل منحني. لكنك إن حققت التفوق في صف حافل بالعباقرة، فلن تخشى شيئاً! لأنك ستنال علامة إيه A».

كان هوفمان قد أدخل ضمن مقرر سي إس 244 تدريس مادة الكريبتوجرافيا، إنما ليس على مستوى عالٍ. ذلك أن أشكال الشيفرة التي تعتمدها الحكومة كانت من الأسرار، بينما كانت تلك الأشكال المستخدمة في القطاع الخاص، بل حتَّى في الجامعات، بدائية نسبياً. ويعترف هوفمان اليوم: لم نكن نتوسع في هذا المجال وتفاصيله. وإني واثق من أنني كنت أدرس شيفرة قيصر وما شابه. ولا تنس أن كل ما كان لدينا يومذاك هو الشيفرات البديلة، والشيفرات المتبدلة، والتجميعات المركبة.

ومنذ اللحظة الأولى التي بدأت فيها الدورة في 1 تشرين الأول/ أكتوبر، بواقع حصتين أسبوعياً، حتَّى 5 تشرين الثاني/ نوفمبر، موعد تقديم أوراق البحث، كان رالف ميركل يميل إِلىٰ التفكير بشكل أكثر طموحاً. إذ ما أن سمع بوظيفة الكريبتوجرافيا من حيث أنَّها وسيلة لحماية المعلومات من تطفّل المتنصتين، حتَّى وجدته يكاد لا يتوقف عن الانشغال الذي ما انقطع الناس منذ عهد يوليوس قيصر عن اعتباره المعضلة الأساس: ابتكار منظومات كريبتوجرافية أكثر منعة، وأقل قابلية للتفكيك مما هو شائع اليوم، ويمكن تشفيرها أَو تفكيك شيفرتها بمفتاح متماثل.

وبدلاً من ذلك، ولأسباب ما تزال غير واضحة، إِلاَّ أنَّها تتصل بطبيعة عقل ميركل غير التقليدي، ركَّز اهتمامه على ما بدا له مظهراً غريباً، وتحدياً لمعضلة أشد جذرية. فقد كان السيناريو الكريبتوجرافي الأساسي، يفترض الضعف في قناة الاتِّصال. وكانت هذه هي الحال حقاً في الإرسال البرقي والبث الإذاعي، وموضوع مادة الدراسة في المقرر الذي يدرسه هوفمان، أي شبكات الكومبيوتر المفتوحة. ولكن ما هي الإجراءات التي بوسعك الإفادة منها، إن شئت الاتصال بشخص لا يملك مفتاحاً متماثلاً مأموناً متفق عليه مسبقاً؟ هل هناك طريقة يستطيع بها هذان الشخصان إجراء حديث مع بعضهما البعض بطريقة عفوية وواضحة لكليهما، ولكنها معماة على من يحاول التنصّت

عليهما؟ وهذه المشكلة، كما بات ديفي وهيلمان يدركان الآن، لم يتصد لها أحد من قبل، لأنها تنأى بلا ريب عن الحل.

أما ميركل الذي لم تفسده المعرفة بنظرية الكريبتوجرافيا أَو تاريخها، فكان لاهياً عن استحالة تحقق المهمة التي يتصدّى لها. وكل ما قام به هو محاولته حل المعضلة وحسب. كان الجانب الحاسم في الوضع يكمن، في رأيه، في اختلاف ظروف الشخصين اللذين أرادا التخاطب فيما بينهما واحتمال وجود متطفل. هنا، ينهمك هذان الشخصان في الحديث بشكل إيجابي بينما المتنصِّت مستمع سلبي. ولقد أدرك ميركل أن الحل يكمن في استغلال التآمر بين المتحادثين، أثناء حديثهما، فينشأ بذلك وضع يستطيعان فيه، كما يقول: «تشويش عقل المستمع السلبي، ولو سمع كل ما يدور بينهما من حديث». وشرع الرجل يقدح زناد فكره في هذا الأمر حتّى كاد أن يستحوذ عليه. وفي إحدى الليالي من تشرين الأول/ أكتوبر 1974، وبينما هو جالس في سريره، في شقته الصغيرة، يحدق في سقف الغرفة، رأى الرجل نفسه وقد وجد الحل الممكن للمعضلة.

أحجيات:

هاك الخطة التي تفتق عنها عقل ميركل في عتمة الليل في غرفته. الوضع التقليدي: يريد بوب وأليس التحادث في أمر ما. بوب هو المرسل وأليس هي الطرف المستقبل لرسالة سرية. ولكن هناك لسوء الحظ متنصّت غير مرغوب فيه، هو إيف التي تستطيع سماع كل ما يمكن أن يدور بين الطرفين. فكيف يمكن لبوب أن يبعث برسالة تستطيع أليس قراءتها، وتعجز إيف عن إدراك فحواها؟ عليه أولاً ابتكار أحجيات كل واحدة منها هي رسالة مشفَّرة جرى تشفيرها بوساطة مفتاح صغير نسبياً، مفتاح يمكن معرفته بقدر مقبول من الجهد في الهجوم بالقوة الغاشمة؛ وهذه مهمّة صعبة إِلاَّ أنه يمكن بالكومبيوتر الذي تملكه أليس. وفي هذا يقول ميركل: «وهذا سبب وصف الأمر بالأحجية،

اللغز، وإنها لمعضلة يصعب حلها، لكن الحل ممكن، بالبحث وتجربة مختلف تركيبات الأَرقام في مدى المفتاح». وبوب لا يبتكر بوساطة الكومبيوتر الخاص به أحجية واحدة فقط، بل الآلاف، وربما الملايين. وهذه كلها ترسل إِلىٰ أليس.

تقوم أليس، في نهاية المطاف، بنشر هذه الأحجيات على الأرض وتختار إحداها عشوائياً. (إيف قادرة طبعاً على اعتراض هذه الأحجيات كلها، لكنها لا تدري ما الذي اختارته أليس منها). ثم تقوم أَليس بمعالجة الأحجية التي اختارتها بأن تجعل كومبيوترها يبحث في مدى المفتاح حتَّى تقع على الحل. ويشتمل هذا الحل على شريط من الأَرقام، إنه الرسالة التي تضمنتها تلك الأحجية بعد تفكيك شيفرتها. هنا يكون حل تلك الأحجية بين يدي أَليس وبوب معاً. إن بوب يعرف الحل، طبعاً، لأن الأحجية من ابتكاره، وهو يملك الحل لكل الأحجيات التي أرسلها. غير أن إيف لا تملك ذلك الحل. ولئن تكن قد اعترضت كل ما أرسله بوب إِلىٰ أَليس، إِلاَّ أنها لا تملك الوقت ولا الكومبيوتر المتطور للعثور على الحلول لهذه الأحجيات كلها، بالإِضافة إِلىٰ أنَّها تجهل الأحجية التي اختارتها أليس.

أما الخطوة التالية لأَليس، فهي إعلام بوب بالأحجية التي اختارتها. وهذا أمر يسير؛ ذلك أن الأحجية المشفَّرة تتضمَّن مؤشراً (إِشارة تقول، مثلاً، «هاك أنا الأحجية رقم 3!»). ومفتاحاً رقمياً طويلاً. وهكذا، حين تعيد أَليس الرسالة، (الأحجية رقم 3)، فإن بوب يستطيع العثور على المفتاح المتضمن في الأحجية. وهنا يكون لدى كليهما مفتاح سرّي يشتركان فيه، ويستطيعان استخدامه في إجراء المزيد من الاتِّصالات السرِّيَّة. وربما تكون إيف قد سمعت بالأحجية رقم 3، لكنها لن تدري أي أحجية من ملايين الأحجيات هي المقصودة. لتتذكر، أن عليها أن تحل كافة الأحجيات حتَّى تبلغ المفاتيح. ولئن يبدو هذا ممكناً باستخدام كومبيوتر عملاق على درجة عالية من التطور، فإنه

يقتضي من المتنصت بذل جهد أكبر مما بذله كل من أليس وبوب، ربما بملايين المرَّات. لكن مقدار الجهد اللازم ليس هو النقطة الهامَّة.

وهاكم النقطة الهامة: لقد استطاع رالف ميركل، في شقة صغيرة في بيركلي، وبعيداً تماماً عن مجال وكالة الأمن القومي، أن يجد طريقة يستطيع بها شخصان، دون اتفاق مسبق بينهما على مفتاح سري، أن يرسلا رسالة سرية، تحبط الجهود التي يبذلها متنصّت مجتهد لتفكيكها.

ورُبّ سائل يسأل عما هي العمليات التي تجري في عقل من يأتي بمفهوم جديد كل الجدة في الكريبتوجرافيا، ذلك المفهوم الذي يدحض التيار الفكري السائد في هذا الحقل على امتداد أكثر من ألف عام؟ ويقول ميركل في هذا: «كان أول ما خطر ببالي، إن هذا الحل عظيم؛ ولعلي أستطيع بواسطته تنفيذ ربع مشروع». ولئن بدا هذا القول بعيداً عن المغالاة، إِلاَّ أنه كان مع ذلك ينم عن مبالغة في التفاؤل. وكان الاتفاق هو أن يعرض ميركل للبروفسور هوفمان، موضوع بحثه أَو «ربع المشروع»، فأسرع بكتابة عرض لما يعتزم القيام بدراسته. وكان ذلك العرض مختصراً بالضرورة ويشوبه الغموض. ويقول ميركل في ذلك مفسراً: «لم أستطع أن أذكر أي دراسات سابقة في الموضوع تقول أن المشكلة هامة وجديرة بالبحث لأنني لم أقع على دراسات سابقة تقول أن هذه المشكلة هامَّة. وحسبت [عن حق] أنه ليس ثمة دراسات سابقة. ولذلك كان ما كتبته بشكل أساسي: مدونة صغيرة». وعلى سبيل الدعم، ذكر [لأستاذه] أنَّه كان يعتزم كتابة بحث في تكثيف البيانات.

بعد أن قرأ لانس هوفمان الاقتراح، قال لصاحبه أنه من الأجدى له الكتابة في مشكلة تكثيف البيانات.

حاول ميركل إقناع أستاذه بأن موضوعه أجدر بالبحث، وأعاد اقتراحه عدة مرات في محاولة لحمل هوفمان على التسليم بأن الموضوع مثير للاهتمام، على الأقل، ليكون جديراً بالمتابعة. لكن هوفمان ظل ثابتاً على موقفه ولم يقبل

حتَّى أن يمنحه تلك المنة البسيطة. فما هو السبب؟ يجيب ميركل: «لأكن مهذباً، وحسبي أن أقول أنه كما يبدو لم يفهم ما كنت بصدد قوله آنذاك. ولذلك انقطعت عن متابعة الدراسة في هذه الدورة».

لم يكن ميركل قد عرف، بعد، بأمر مارتي هيلمان. لكنَّه كان يريد شخصاً ما، أي شخص، ليطمئنه بأن ما أملته عليه فطرته كان صحيحاً، وأنَّه وقع على أمر ذي شأن. غير أن ردود الفعل التي قابله بها الأكاديميون في بيركلي، كانت مماثلة لما بدر من هوفمان: «كان القوم بصورة أساسيَّة يحدِّقون في وجهي مستغربين ما كنت أقوله أشد الاستغراب، وحجتهم في ذلك أن الموضوع، على ما يبدو، غريب جداً. وأخيراً، قدَّم له أحد أساتذته، ويدعى روبرت فابري، بعض التشجيع، وقال له إن الفكرة جيدة، فحاول أَن تقوم بنشرها. وهكذا التفت ميركل إِلىٰ بحثه وأعاد صياغته بشكل أكاديمي أفضل، آملاً أَن ينشر في مجلة [جمعية الآلات الحاسبة] كوميونيكيشنز أف ذي إيه سي إم ACM ذات المكانة الرفيعة. وقد جعل عنوان بحثه «اتِّصالات مأمونة عبر قنوات غير مأمونة»، وقدَّم موضوعه رسمياً في آب/ أغسطس 1975، إِلىٰ رئيسة التحرير: سو جراهام.

وفي 22 تشرين الأول/ أكتوبر 1975، وجهت جراهام رسالة إِلىٰ ميركل قالت فيها أن «خبيراً متمرساً في الكريبتوجرافيا قد اطلع على البحث المقدم ووجده غير صالح للنشر. (لم تذكر الرسالة اسم القارئ، أَو القارئة، جرياً على عادة إغفال الاسم، لكن القراء يتم اختيارهم عادة من بين الراسخين في حقلهم العلمي). وكان العيب الظاهر في ذلك البحث، وفق قول ذلك القارئ، هو عين الفرضية التي يقوم عليها، أي القول أنه من الممكن قيام نظام كريبتوجرافي دون ضمان تسليم المفاتيح. وهكذا إذن، فإن ما جعل فكرة ميركل ثورية هو نفسه ما جعلها مرفوضة أيضاً. وقد عبَّر القارئ عن رأيه بالقول: «إني آسف لإعلامكم بأن البحث لا يتفق والرأي السائد الآن في الفكر

الكريبتوجرافي. والتجربة تبين أن من الخطورة بمكان تداول معلومات جوهرية علناً». ولقد تكلفت سو جراهام ذاتها جهداً عظيماً لتؤكد اتفاقها في الرأي والقارئ، فنطالعها تقول في رسالتها: «لقد قرأت التقرير شخصياً وأزعجني فيه خاصة خلوه من الإِشارة إِلىٰ المراجع. أفليس هناك شخص آخر عالج هذا النهج [؟]».

وإن الجواب فيما يتعلّق بالبحوث المنشورة حصراً، هو بالنفي.

انتاب ميركل يومئذ شعور بخيبة الأمل، لكنَّه لم يشعر بالهزيمة. ولعله لم يكن متفاخراً متهوراً مثل والده، الذي وُصف ذات مرة بأنه «مزيج مثالي من عالم الفيزياء والبائع الشاطر»، وعرف بمزاجه العصبي ودخوله بسيارته الباكارد المكشوفة المتعبة ساحة الوقوف لمختبر ليضرمور بسرعة كبيرة. غير أن الشاب ورث عن أبيه روح الدأب والمثابرة. وراح يشذِّب في مقاله وينقّح ولم ينقطع عن ذلك بالرغم من رفضه من عدة دوريات. ويقول في هذا: إن الملفت في الأمر كيف أن عملية النشر كانت تؤدي إِلىٰ تحسينات متزايدة، إِلاَّ أنَّها كانت سيئة جداً في تناول موضوع يختلف كل الاختلاف عن المعهود». لكنَّه كان واثقاً من أن الفكرة التي عرضت له كانت جديرة بالمتابعة: «لا يمكن أن تكون الفكرة خاطئة لأنها بسيطة. ولم يكن من الواضح إِلىٰ أين ستقودنا، إِلاَّ أنه كان واضحاً جداً بضرورة عرضها. وكنت أريد بشكل أساسي نشر تلك الفكرة والإعلان [على الملأ] هاكم فكرة بسيطة، وهي توضح طبيعة المشكلة وتبين حقيقة أن لها حلاً ممكناً، وأنَّها باتت الآن مشكلة بحث محددة. لندعُ بعض القوم إلينا، ولنر عندئذ أي جديد سوف يتمخض عنه بحثنا».

في أوائل عام 1976، وكان ميركل قد بدأ يشعر بالإحباط، أخبره زميل له أنَّه يعرف بعض الأشخاص الذين يشاطرونه اهتمامه، وأبرزهم مارتي هيلمان. وجدير بالذكر أن من بين المواد التي كان هيلمان يقوم بتدريسها، مادة تبث عبر دارة مغلقة ما بين ستانفورد وبيركلي. وقد استطاع ميركل

الاستماع إِلىٰ إحدى الحلقات المذاعة، وأدرك فوراً أن مارتي هيلمان كان بالفعل يشاركه التفكير في الأمور ذاتها التي تشغل فكره. وفي الوقت الذي أخذت فيه مسودة البحث الذي وضعه ديفي وهيلمان حول «أساليب كريبتوجرافية لعدة مستخدمين» توزع على البعض قبل أن تُنشر، استطاع ميركل الحصول على نسخة منها. وبدلاً من الشعور بالضيق لأن هناك من سبقه إِلىٰ نشر هذه الأفكار، انتابه إحساس بالغبطة لكون تصوره بات موضوعاً يطبّق فعلاً. وكان أن حفزته الفكرة عند اطلاعه على البحث أن يسعى للانضمام إِلىٰ الباحثين في جامعة ستانفورد؛ وهذا ما جعله يوجه رسالته إِلىٰ هيلمان المؤرخة في 7 شباط/ فبراير والتي اقترح فيها قيام تعاون بينهما، مرفقاً بها مسودة بحثه، بدلاً من نبذة عن حياته.

كان بحث ميركل كشفاً بالنسبة لديفي وهيلمان، إذ لم يكن ليخطر ببال أي منهما أنه سيرى أفكارهما تطبق حقاً قبل مضي فترة من الزمن. ورأى الرجلان في تصور الأحجية، الذي بلغه ميركل تطوراً مؤكداً، وإن كانت تعتوره المشكلات. وهكذا سرعان ما غدا ميركل جزءاً من النقاش بين ديفي وهيلمان حول تطبيق المفتاح العام. ولقد تساءل ميركل كيف يمكن لفكرة الأحجية التي خرج بها أن تندمج وذلك الضرب من المفتاح العام الذي أخذ به ديفي وهيلمان في إطار منظومتهما الكريبتوجرافية. ثم اقترح في رسالة مؤرخة في 2 نيسان/ أبريل 1976 منظومة تسمح بأن يكون لكل مستخدم مجموعة خاصة فريدة من الأحجيات ـ وتكون هذه في ذاتها المفتاح العام. «وهكذا إذا شاء أحدهم أن يبعث برسالة إِلىٰ الجهة ألف A فما عليه إلاّ أن يختار عشوائياً إحدى أحجياتها. ثم يعمد إِلىٰ تشفير الرسالة وإرسالها إِلىٰ الجهة ألف A. وتقوم الجهة ألف بفحص مفتاح الأحجية مستخدمة بطاقة الأحجية على وجه الرسالة. ولو أراد سواهم قراءة الرسالة لما استطاع، لأنه لا يملك معرفة مفتاح الأحجية». كما كتب ميركل.

ولقد قام ميركل بالتفكير في كيفية الاستفادة من الأحجيات المندمجة في

نظام المفتاح العام، في تلقي الإيصالات باستلام الرسائل. ولما بلغ هذا الحد، جعل من فكرته هذه طعماً مغرياً، وأسر بأنّه يبحث عن عمل في فصل الصيف. وأشارت جملة الختام في رسالته إِلىٰ المثلب العملي في منظومته، أن مستوى الأمان الذي توفره الأحجيات، إنما كان على المستوى الحدودي رياضياً Polynomial، وليس على المستوى الأسي Exponential الأشد صرامة. وإذن، فإن على المتنصت أن يجهد نفسه كثيراً حتّى يتمكن من حل الأحجيات، لكن عامل الجهد ذاك كان محدوداً بعدد الأحجيات. ولنفترض أن أليس أرسلت إِلىٰ بوب؛ وفق نظام الأحجيات المشفَّرة، مليون أحجية ليختار منها المناسب، غير أن المتطفلة إيف، كان لديها كومبيوتر أسرع في إجراء العمليات الحسابية ألف مرة من ذاك الذي يستخدمه بوب. (ليس في هذا الافتراض مبالغة، إذا أخذنا بعين الاعتبار، أن ثمة حكومات غنية، ولديها موارد كومبيوترية ضخمة، وربما رغبت بفك الرسائل المشفَّرة التي يصدرها أَو يتلقاها هذا الطرف أَو ذاك). وقد تتمكن أَليس من حل ألف أحجية، في حين أن بوب يستغرق الوقت ذاته لحل أحجية واحدة مختارة عشوائياً. فإذا احتاج بوب إِلىٰ دقيقة لحل أحجية واحدة، فإن أَليس تحل مليون أحجية في حوالي ست عشرة ساعة، وهذا وضع لا يحتمل إطلاقاً بالنسبة لأولئك الذين يحتاجون حماية قوية. وحتّى لو كان كومبيوتر أَليس لا يزيد قوة عن الكومبيوتر الذي يستخدمه بوب، فإن أَليس تستطيع حل كل الأحجيات في أقل من عامين. وإذا كان الحفاظ على السرِّيَّة ضرورياً، فإنَّه ليس بالمرغوب، أيضاً. (من جهة أخرى، فإن مثل هذه المدة كافية للتحقّق والتثبت، طالما أن معرفة مفتاح التوقيع بعد عام من استخدامه لن يوفِّر للعدو أي ميزة ذات شأن). إن أي نظام تشفير يعتد به، عليه أن يكفل ـ مهما تكن الدالة الوحيدة الاتجاه المستخدمة ـ وجود علاقة أسية، رياضياً، بين الحسابات السهلة للمرسل والمهمة الأصعب المفروضة على المتنصت. وهذا كفيل، من الناحية المثالية، بزيادة حجم عمل الخصم إِلىٰ حد يتطلب آلاف، أَو ملايين أَو مليارات السنين لإنجاز المهمة. وكان ميركل يأمل بالتوصل إِلىٰ

طريقة تجعل منهجه يفي بهذه الشروط. فكتب إِلىٰ هيلمان يقول: «ربما نستطيع أن نصل إِلىٰ الأسية في نهاية هذا الصيف».

بينما كان ميركل يقدح زناد فكره بحثاً عن طريقة للوصول إِلىٰ الأسية، كان اهتمام ديفي وهيلمان منصباً على ابتكار طرقهما الشخصية لتنفيذ منظومتهما الخاصة بالمفتاح العام للشيفرة. ذلك أنّه إذا لم تتوفّر لهما طريقة ما لوضع أفكارهما موضع التطبيق أَو على الأقل إثبات إمكانية وجود خطة عملية لذلك فلسوف يبدو تصور المفتاح العام للشيفرة مجرد حيلة من حيل العقل الرياضي.

وكانت إحدى تلك الطرق، ما عرضه دونالد كنوث: عالم الكومبيوتر في جامعة ستانفورد، والذي أكسبته سلسلة كتبه الموسوعية «من برمجة الكومبيوتر» The Art of Computer Programming، التي ما زالت أجزاؤها تتالى، سمعة واسعة باعتباره حجّة الخوارزمية الأكبر. فقد ذكرهما كنوث بظاهرة رياضيَّة طريفة: ففي حين أن ضرب عددين أوليين ببعضهما عملية بسيطة كلعب الأطفال، فإن عكس هذه العمليَّة ـ وتدعى التحليل إِلىٰ عوامل ـ قد تسبِّب الحيرة للشيطان ذاته. فهل تصلح هذه الظاهرة أساساً لدالة (تابع) وحيدة الاتجاه شيطانيَّة يصعب اختراقها؟ ولئن لم يشأ ديفي وهيلمان متابعة هذه الفكرة فإن هناك آخرين اتبعوا هذا الطريق.

كان ثمة حل آخر ينطوي على تعقيد حسابي، التفت إليه ديفي وانقطع لقراءة كتاب مكرس له، وخاصة الفصل المتعلق بما كان يسمى دوال (توابع) إن بي الكاملة NP Complete functions، وكتب ديفي فيما بعد، يصف تلك التوابع بأنَّها «مشكلات لم يكن يعتقد بأنَّها قابلة للحل في وقت حدودي بأي كومبيوتر محكم». وكان مؤدى ذلك بأن هذه المسائل هي من الصعوبة بحيث تجعلك تتخذ كومبيوتراً من طراز ماكنتوش أَو حتّى كومبيوتراً عملاقاً من طراز كراي Cray (إذا كنت وكالة الأَمن القومي) لتتمكن من حل المعضلة، وإذا ما عدت

للتحقق من النتائج بعد بضعة تريليونات من السنين، وجدت نفسك ما تزال بعيداً بُعداً شاسعاً، عن الحل. ولئن كان ديفي يحمل بعض الأفكار للإفادة من الحسابات المركبة في وضع صيغة لدالة كريبتوجرافية وحيدة الاتجاه فإنَّه لم يقيض له إيجاد طريقة لتنفيذها مع الأبواب السحرية.

ولقد تجلّى الأمل باقتراح من أحد زملاء هيلمان في قسم الهندسة الكهربائية، في ستانفورد، ويدعى جون جيل، إذ لفت الانتباه إِلىٰ عملية رياضية تُعرف باسم «الأسية المتفردة» كتابع محتمل. ولما كان عكس هذه العملية، والمعروف (باللوغاريتم المتفرد) عملية بالغة الصعوبة، فإن هذه المسألة حملت معها إمكانية تحقيق المعيار الأساسي للدالة (التابع) الوحيدة الاتجاه: أعداد بسيطة يتسلى الأخيار بحسابها، وجحيم حسابي للأشرار الذين يريدون عكس العملية.

كان ديفي يعمل في مختبر الذكاء الاصطناعي في جامعة ستانفورد في أحد أيام أيار/ مايو 1976، لإعادة صياغة البحث حول المفتاح الكريبتوجرافي العام، والذي كان يعده مع مارتي للنشر، في وقت لاحق من العام، في مجلة مؤسَّسة مهندسي الكهرباء والإِلكترونيات البارزة آي إي إي إي IEEE، حين اتصل به هيلمان ليخبره بصوت منفعل أنَّه يعمل على الأسية المتفردة، وأنَّه توصَّل فعلاً إِلىٰ نظام عملي للمسألة. ولما مضى في الشرح أدرك ديفي فوراً أن هيلمان استطاع ربط الخطوط المتشابكة لنظرية كانت تدور في رأسه طوال أَسابيع.

ولقد قُيض للخطة المقترحة أن تُعرف باسم خوارزمية ديفي ـ هيلمان. وتقوم على الافتراض بوجود طرفين يريدان الاتصال سراً؛ وأن بإِمكان هذين الطرفين توليد مفتاح مشترك معاً، باستخدام الدالة (التابع) الوحيدة الاتجاه، ولا يملك المتنصّت معها اعتراض المحادثة. وهاكم طريقة العمل:

يختار الطرفان أولاً رقمين. ويتم هذا علناً، لأن معرفتهما لن تفيد المتنصّت. ثم يختار كل طرف رقماً سرياً خاصاً به، ولا يكشف عنه أَو يرسله

إلىٰ أحد. ثم عن طريق استخدام صيغة رياضية تتصل بالأسية (الرفع إلىٰ القوة الجبرية)، يأخذ كل منهما رقمه السري الخاص به، ويقوم بعمليّة حسابية قوامها ذلك الرقم السري والرقمان المعلنان اللذان سبق اختيارهما. وبعد عملية السحق الرقمية القصيرة هذه يكون لدى كل منهما رقم سري متحوّل ويرسل هذا إلىٰ الطرف الآخر. وليس في إرساله عبر قناة مفتوحة أي مشكلة لأنه، في النهاية، رقم سري مشفّر، تمّت تعميته بوساطة الدالة الوحيدة الاتجاه وهو سهل التنفيذ إلاّ أن عكسه بالغ الصعوبة (ما مقدار صعوبته؟ إن فكّ العملية هو، نظرياً على الأقل، صعب كحل مسألة اللوغاريتم المتفردة. وهذا يقتضي إجراء مليون كوادريليون عملية رياضية أكثر من عمليات الأسية المستخدمة في تحويل الأعداد. تلكم هي الدالة الوحيدة الاتجاه!).

وبمقدورك اعتبار هذا الزوج الثاني من الأعداد بمثابة المواليد التي نتجت عن الأرقام المعلنة المتفق عليها صراحة على الملأ والأَرقام السرّيّة المكتومة. ومحاولة استخلاص الرقم السري من الرقم الذي يجري في القناة المفتوحة أشبه بفحص الحامض النووي DNA في الخلية البشرية ومحاولة اكتشاف مساهمة كل من الأبوين في تكوين كل جينة على حدة. وهذا ما لن تقدر عليه ما لم يكن بوسعك الوصول إلىٰ الحامض النووي، إما من السائل المنوي أَو من خلايا البويضة.

يقودنا هذا إلىٰ الخطوة الثالثة والأخيرة من خوارزمية ديفي ـ هيلمان. هنا يعتمد كل من الطرفين صيغة رياضية خاصة تجمع بين هذه الأرقام المتحولة مع الأرقام السرية الأصلية (الحامض النووي الأصلي!) الخاصة بالطرف الذي يقوم بالعمليّة للوصول، إلىٰ رقم آخر. وهذه الصيغة تعمل بحيث يتوصل كلاهما إلىٰ رقم نهائي متماثل، بالرغم من أن الأعداد الأصلية لديهما مختلفة عن بعضها البعض. ويمكن تسمية هذا الرقم المتماثل «م»، الحرف الأول في كلمة مفتاح. وهكذا يكون قد أصبح كل منهما مالكاً الآن لمفتاح رقمي مماثل لمفتاح صاحبه

ومصمّم على نحو لا يستطيع شخص آخر الوصول إِلىٰ «م»، إلاً إذا كان لديه أحد الأَرقام السرية الأصلية. والمتنصت لن تتوفر له، الفرصة لمعرفة الأَرقام السرية؛ ولن يملك ذاك الخصم إلاً الصيغ المتغيرة التي يكاد يكون من المستحيل الاهتداء إليها.

لقد كانت خوارزمية ديفي ـ هيلمان أشد كفاءة وأماناً من نظام الأحجيات لميركل. لكن تلك الخوارزمية ظلّت دون التطبيق التام لذلك الطراز الذي كان يراود خيالهما من نظام المفتاح العام للشيفرة. ذلك أن ديفي وهيلمان لم يأخذا موضوع التوقيع الرقمي في حسبانهما، كما أنهما لم يوفرا الوسائل لتشفير الرسائل. إِلاً أن النظام الذي أتيا به، وفّر منهجاً يستطيع به من لم يسبق لهما التخاطب من قبل، استخدام قناة مفتوحة، ويحصلا على مفتاح سري. ويمكن استخدام هذا المفتاح في نظام تشفير تقليدي، مثل معيار تشفير البيانات لتعمية الرسائل، ثم تفكيك شيفرتها. (وأسلوب الخزان المزدوج هذا، طريقة للوصول إِلىٰ مفتاح دون اتفاق مسبق، وطريقة أخرى للتواصل فيما بينهما سراً، عرف فيما بعد باسم «الهجين»).

وكان من شأن إدخالهما خوارزميتهما الجديدة إِلىٰ بحثهما «أساليب لعدة مستخدمين» بعد تنقيحه أن جعلت منه وثيقة أشد وقعاً من البحث ذاته في صيغته الأصلية. ثم قدّم البحث الجديد «اتجاهات جديدة في الكريبتوجرافيا» بتاريخ 3 حزيران/ يونيو 1976. وفي وقت لاحق من الشهر ذاته، عرضا بعض أفكارهما أمام مؤتمرين أحدهما في لينوكس بولاية ماساتشوسيتس والآخر في رونيبي في السويد، وقد قدر أن يكون لمشاركتهما عواقب لم يتعمداها، وتتصل بحقوق الملكية الفكرية. والحقّ، أن استغلال الملكية الفكرية كان آخر ما يخطر ببال هذين العالمين في حقل المعلوماتية. وعلى الرغم من العراقيل التي صادفاها بسبب رفض الحكومة توفير كافة التفاصيل المتعلقة بمعيار تشفير البيانات، كانا يعملان على ابتكار بديل علني كامل للكريبتوجرافيا ذاتها.

وفي تلك الأثناء، كان رالف ميركل، الذي بات الآن يتقدم في دراسته، لنيل الدكتوراه في علم الكومبيوتر من جامعة كاليفورنيا في بيركلي، قد سلم أخيراً بأن مشروع الأحجيات ما زال بحاجة لكثير من الجهد. فبدأ عندئذ بالبحث عن منهج آخر لتنفيذ المفتاح العام. وقد عبّر عن هذا الوضع بقوله: «كان لدي خطط مختلفة تشتمل على دوائر وألعاب معقّدة، ومختلف أشكال المجموعات الجزئية». لكنها جميعاً لم تحقق له المطلوب. ومما زاد في عجزه الصعوبة المزمنة التي يعاني منها في التعبير بوضوح عن الأفكار المعقّدة؛ وهذا ما جعل من العسير على زملائه الإشارة إليه بإجراء تعديلات على مشاريعه. وقد برَّر ميركل ذلك في دفاعه بالقول: «إنك مضطر لأن تمد عقلك، فإذا بأمور غريبة عجيبة معقدة تداهمك أحياناً، ولا تستطيع عندئذ أن تعمل فيها تبسيطاً، إلاً بعد أن تكون الفكرة قد نضجت، إلىٰ الحد الذي تصبح فيه نقية ويسهل عرضها بوضوح».

لبَّى هيلمان عرض ميركل بالعمل معه، وقدَّم له عملاً في البحث أثناء فصل الصيف. وإنه لأمر ينعش القلب أن يعمل المرء مع الشخصين الوحيدين في العالم اللذين يدركان المشكلة على الوجه الأفضل. وقد وصف ميركل حاله يومذاك بقوله: «كنت منعزلاً حتَّى التقيت هويت ومارتي. وكنت مستعداً لأن استمر في الضرب بقوة حتَّى تتحقَّق لي استجابة ما، إلاً أنه لم يكن هناك من يهتم بمتابعة المشكلة». ولقد حل ميركل في ستانفورد وهو مقتنع بأن فكرته الواعدة تدور حول خطة للعثور على التوابع الوحيدة الاتجاه للباب السري بالاستناد إلىٰ مسألة توابع إن بي الكاملة. وهذا النظام يقوم على مسألة رياضية تُعرف بالحقيبة Knapsack. ولاستيعاب هذه الخطة تدخل، حقيبة، وكما يقول ميركل: «إن أساس الفكرة. هي أن تضع الأشياء في الحقيبة، بحيث تمتلئ حتَّى أطرافها دون زيادة أو نقصان». ووصف ديڤي هذه المسألة بأنَّها شبيهة بحال موظف الشحن الذي يجد أمامه مجموعة من الرزم المختلفة الأشكال

والأحجام ويضطر معها لإيجاد أفضل طريقة لإدخالها في حقيبة البريد. والحل المثالي هو الذي يسمح بحشو الرزم واستغلال كل بوصة من الفراغ. والحق أنَّه من الأصح القول، حسب خطة ميركل، أن على الموظف معرفة الترتيب المناسب لوضع الرزم. بحيث تتفق وحدود الوزن المسموح للحقيبة أن تستوعبه. وإذا كان عدد الرزم قليلاً، فلن يكون من الصعب التوصّل إِلىٰ الحل المثالي، لكن المسألة تغدو أصعب إذا كان عددها كبيراً.

وبما أن ميركل أراد من هذه الحقائق تأدية دور الدالة الوحيدة الاتجاه للباب السري، وهذا أمر يسهل على الشخص المناسب حله، لكنَّه يكاد يكون من المستحيل على أي شخص آخر تفكيكه، فقد كان عليه إيجاد طريقة لتذليل هذه المعضلة لصاحب المفتاح الحقيقي. واستطاع تحقيق ذلك بواسطة شكل أسهل من مسألة الحقيبة هو الحقيبة المنتفخة. وفي هذه المسائل، يجري ترتيب الأوزان بشكل يجعل اكتشاف الحل ضرباً من التسلية. واكتشف ميركل طريقة تحول هذه العمليات السهلة إِلىٰ مشكلة الحقيبة العادية الأشد تعقيداً، حيث يجري ترتيب الأوزان على نحو ليس فيه ذلك النوع من اليسر.

كانت تلك عملية معقَّدة، إِلاَّ أنَّها منطقيَّة. وأساس ذلك أنَّه إذا أراد شخص ما أن يتلقَّى رسالة خاصة، فعليه البدء بحقيبته المنتفخة، وهي بالضرورة مفتاحه السري. ثم يكون له استخدام ذلك المفتاح لصنع الحقيبة العادية العسيرة على الحل لتكون المفتاح العام. واعتماداً على هذه الصيغة التي ابتكرها ميركل (وهو يعمل مع هيلمان) أمكن جعل الحقيبة الثانية تقوم بوظيفة تشفيرية بجعل الرسائل معماة على نحو لا يمكن إعادتها إِلىٰ ترتيبها الأصلي إِلاَّ على يد شخص لديه المقدرة على حل مشكلة تلك الحقيبة الثانية. وهذا يعني، عملياً، أن ثمة طريقة وحيدة لتنفيذ هذا الأمر، وهي استخدام المفتاح السري، وهو الحقيبة المنتفخة (اليسيرة على الحل).

أما الطريقة غير العمليّة فهي إنفاق بضعة مليارات من السنين في حل المشكلة بالهجوم بالقوة الغاشمة.

هل هناك طريقة ما للتغلّب على النِّظام أكثر بساطة من استخدام الكومبيوتر ذات القدرات الفائقة في الهجوم الشامل بالقوة الغاشمة، بأمل الحصول على المفاتيح قبل انقضاء النهار؟ أو بعبارة أخرى هل يستطيع محلِّلو الشيفرة أن يجدوا طريقاً مختصراً، أَو ضعفاً يستغلونه للوصول إِلىٰ المفتاح السري؟ الحق أن ميركل كان شديد الثقة بأن النِّظام خال من كل ضعف، وقد بلغت به الثقة أنّه علق على باب مكتبه إعلاناً. ثم كتب إِلىٰ هيلمان: «إنّي أعرض جائزة 100 دولار لأول شخص يتمكّن من اختراق النِّظام. وقد أطلعت عليه بعض الأشخاص هنا، وخلصت بعد الإصغاء إِلىٰ الصمت، إِلىٰ أن الحل، إن وجد، هو على الأقل ليس بالبسيط الذي يُستهان به». وعمد، لتزويق الأمر، إِلىٰ تبسيط المهمة إِلىٰ حدّ عظيم بأن طلب إِلىٰ عدد من المعنيينْ بفك الشّيفرة حل المعضلة بعد تخفيض مستوى صعوبة مسألة الحقيبة إِلىٰ الحد الذي كان ميركل يعلم معه أن ثمة، على الأقل، احتمالاً بعيداً بأن يتمكن شخص ما من الفوز بالجائزة. ثم يعمد بعد ذلك، إِلىٰ رفع قيمة الجائزة إذا استطاع أحد حل المسألة كما وضعها. ولكن ما حصل، على حد وصفه: «لم أجد أحداً يهتم بالموضوع. وقد حسبت أن المهتمين سيتدافعون إِلىٰ حل المشكلة إن عرضت مالاً للحقيبة [العصية على الحل، احتمالاً]، لأن الاحتمال قائم بأن يتمكن أحد من معالجتها فعلاً، أَو يعتقد على الأقل، بأن ثمة احتمالاً بإمكانية حلها». (وقد وضع بحثاً مع هيلمان في عام 1978، حول نظرية الحقائب).

وفي تشرين الثاني/ نوفمبر، نشر بحث ديفي وهيلمان «اتجاهات جديدة في الكريبتوجرافيا» في مجلة آي إي إي إي IEEE وكان اكتشافاً، وضربة حقيقيّة تنزل بالإِمبراطورية. (استوحى الكاتبان العنوان من جذور جيلهما، مستذكرين دار النشر التي تسمى الاتجاهات الجديدة والتي تصدر طبعات شعبية لكتب ذات

مستوى فكري رفيع، وتعتبر من الكتب المقدّسة عند أبناء جيل التمرد مثل «بانتظار جودو» و«سيد هارتا»). وقد استهل الكاتبان مقالهما بعبارة مدوية: «إننا نقف اليوم على عتبة ثورة جديدة في الكريبتوجرافيا». وآية ذلك أن عصر الكومبيوتر يسمح بتطبيقات زهيدة التكاليف لأدوات التشفير، وهي أدوات ضرورية لعالم يقدم وسيلة «للاتّصال بين الناس أَو بين أجهزة الكومبيوتر عبر العالم، لا تكلف جهداً وتتميّز برخص الثمن». لكن الكريبتوجرافيا التقليديّة لا تستطيع، بسبب مشكلة توزيع المفتاح، وعدم توفّر عنصر التوقيع الرقمي اللازم، أن تعالج هذه التحديات: «فاستخدامها سوف يكلف مستخدمي هذا المنهج من أسباب الضيق الشديد، ما يذهب بالكثير من فوائد المعالجة عن بُعد». وهكذا نرى أن ثمة حاجة لأمر جديد، وسيلة يمكن بها إجراء وتبادل المحادثات فعلاً بين أطراف ليس بينهم لقاء سابق، والتثبت من صحة التواقيع لتوثيق المخاطبة بين المرسل والمتلقي، مع السماح بالتوقيع الرقمي. إن ديڤي وهيلمان لم يكونا أول من عرض هذه المعضلات بصورة منهجية واضحة، من فوق المنابر وحسب، بل قاما أيضاً فيما بعد بعرض الحلول لها بواسطة المنهج الذي ابتدعاه، المفتاح العام لأنظمة الشيفرة.

ولقد راودت ديڤي ذات يوم أحلام صورت له وضع مدونته عن الاكتشاف العظيم في الكريبتوجرافيا، لا في صورة البحث الأكاديمي، بل بشكل رواية جاسوسية. فلطالما خاب أمله في الكتب التي تنتمي إِلىٰ هذا النوع من الأدب، والذي يتضمن في حبكته اكتشافات تقنية ذات شأن، وكان مصدر خيبته افتقار تلك الروايات للإقناع عند تصوير الفتوحات العلمية التي تعرض لها؛ فهي تقوم، حسب وصفه، على «أقدام من صلصال». ويتابع ملاحظاً: «وجدت نفسي لسوء الحظ، أني حين توفر لي الاكتشاف العلمي، لا أدري كيف أكتب رواية، وكان علي إقناع نفسي بالنشر في المجلات العلمية الاختصاصية، مثل كل إنسان آخر». ولكن حسبه من ذلك أن البحث الذي نشره مع مارتي هيلمان

كان مشوقاً كأي رواية من مستوى أكثر الكتب رواجاً على مدى الزمن. وكان هذا هو العلم الذي اخترق الحواجز التي لم تبلغها روايات الخيال العلمي، حتّى ذلك الحين؛ ففي صيغها الرياضيّة كان مخطط الاتّصالات في القرن الحادي والعشرين.

اختتم ديفي وهيلمان بحثهما بالملاحظة أنه طوال تاريخ الشيفرة كان الهواة هم غالباً الذين يأتون بالجديد في الكريبتوجرافيا. وذكر توماس جيفرسون الذي ظل ابتكاره لجهاز دولاب التشفير يستخدم طوال قرنين بعد ذلك، كما أنّهما ذكرا الهواة الأربعة الذين خرجوا، كل على حدة، بتطبيقات الآلات الإلكترونية الدوارة التي غلب طابعها على أجهزة الشيفرة من طراز إنجيما، أثناء الحرب العالمية الثانية. ثم أنهيا المقال بالتعبير عن أمنية بأن تكون جهودهما بداية مجهود يبذل لتغيير مشهد الكريبتوجرافيا الحديثة: «إننا نأمل بأن يلهم هذا آخرين (سوانا)، للعمل في هذا المجال الساحر الذي كانت المساهمة فيه تلقى الردع حتّى الماضي القريب [تحت تأثير] احتكار الحكومة التام تقريباً».

ولقد تحطّم هذا الاحتكار على يدي متسلل سابق في معهد ماساتشوسيتس ذي شعر طويل مسترسل ومستشاره ذي المزاج العاطفي، خريج جامعة ستانفورد.

البداية

«هاك شيئاً مثيراً للاهتمام. . .»

كانت هذه عبارة عارضة وردت في بحث أرسله طالب يحضِّر لنيل شهادة الدكتوراه، إِلىٰ أحد الأساتذة الجامعيين. ولم يكن لرون رايفست، الأستاذ المساعد في معهد ماساتشوسيتس للتكنولوجيا ذي التاسعة والعشرين عاماً، ما يحمله على الاعتقاد بأن هذا البحث أكثر مدعاة للاهتمام من مئات أوراق البحث والمقالات المنشورة والمذكرات التقنية التي وقع عليها في عهده القصير بالعمل الجامعي. وكان أحد مؤلفي البحث، وهو هويت ديڤي، قد عمل في المبنى ذاته الذي يعمل فيه، تيك سكوير في كامبردج، حيث يقوم مختبر الذكاء الاصطناعي في الطابق الذي يعلو مكتب رايفست في مختبر علوم الكومبيوتر. لكن: لا اسمه ولا اسم شريكه في البحث، مارتين هيلمان، كان مألوفاً لديه. بل الحق أن رايفست لم يكن ليعرف إِلاَّ القليل عن التشفير، ويجهل مبلغ حساسيَّة الموضوع. وفضلاً عن ذلك أنَّه لم يجد في البحث أي فتح جديد في الفكر الرياضي؛ ذلك أن المعادلات فيه خلت من كل أثر لروح الرياضي الفرنسي بيير فيرما».

ومع ذلك، فإن رون رايفست، وجد في «اتجاهات جديدة في

الكريبتوجرافيا» أكثر من مجرد بحث طريف، بل الحق أنّه وجده مشوقاً، وفي النهاية أحدث انقلاباً في حياته.

لقد استهوت المقالة قلب رايفست وملكت عقله. وجدير بالذكر أن الرجل كان يعنى بالنظريات، سوى أنَّه لم يكن بالمنظّر الذي يرضى بالمجردات البسيطة ويقف عندها. فالمثالي لديه من يفيد من لطائف الفكر الرياضي في التطبيق، ويحدث تغييراً محسوساً في عالم الواقع الحقيقي المُعاش. ووجد أن الإنطلاقة التي جاء بها ديڤي وهيلمان تزاوج بين التجريد والواقع، بالإِفادة من صيغة رياضيَّة مبتكرة لتلبية حاجة اجتماعية. وشاء بعد هذا الاكتشاف تمضية حياته في هذا المجال حيث التقى هذين العالمين.

لئن كان رايفست يمتلك موهبة عظيمة في الرياضيَّات، إِلاَّ أنّه لم ينشأ نشأة الرياضي الكلاسيكي المهووس بالأرقام. كان والده مهندساً كهربائياً يعمل في مختبر شركة جنرال إلكتريك في شناكتادي في نيويورك، وهناك أفاد من مناهج العلوم القوية التي تدرس في المدرسة الثانوية الحكومية حيث تلقَّى علومه. والتحق في فصل الصيف بدورة دراسية تخصّصية في الرياضيات في كلاركسون كوليج. إِلاَّ أنَّه بدأ يميل، وقد اقترب موعد امتحانات الشهادة الثانويَّة، إِلىٰ دراسة علم النفس أَو القانون. وكان مبرزاً في الرياضيَّات مما سمح له بدراستها في جامعة ييل، لكنَّه يبرِّر دراسته للرياضيات أنَّها: «كانت قليلة المتطلبات للدراسة فأتاحت لي دراسة الكثير من المواد الأخرى». وكان من بين تلك المناهج، الكثير من الحصص في علم النفس والتاريخ والموضوعات الأخرى التي لا يحتاج فيها المرء لاستخدام المسطرة الحاسبة. لكن الرياضيات، كما يقول، «إنما كانت موضوعاً من موضوعات كثيرة كنت أشتغل بها».

إن رايفست يتحدّث في هذا الأمر، كعهده دائماً، بنبرة هادئة، رصينة، متأنية، عميقة، توحي بالتفكير فتشد إليه المستمع. وهو رجل أقرب إِلىٰ

الصلع، وجهه مستطيل الوجنتين ترتاح العين لمرآه، وذو لحية مشذبة بشكل حسن؛ وليس في مظهره قطعاً ما يوحي بأن الرجل ينطوي على تهديد للأمن القومي. ولئن كان صاحبنا قد شارك وهو على مقاعد الدراسة في ييل في بعض مسيرات الاحتجاج على الحرب في الفييتنام، فإنَّه كان أبعد ما يكون عن المعارض النشط، الذي يجعل شاغله تأجيج العواطف. بل، ولم يكن ليخطر له ببال حقاً أن يقوم بعصيان أو يحرض عليه.

في ييل، اكتشف رايفست علم الكومبيوتر. فقد أدرك يوم كان يحضر المناهج التي يوفرها قسم الهندسة أن البرمجة توفر فرصة لدمج النظرية بالعمل، والإتيان بأثر ملموس ذي شأن، وكان أن وقع في هوى ذاك الشكل من الفعل الذي يأتي بالجزاء فوراً. ولقد أفاد يومئذ من مهاراته في البرمجة بالعمل بدوام جزئي لدى أحد أساتذة الاقتصاد الجامعيين؛ وإذ وجد نفسه يعمل يومئذ بأحد كومبيوترات آي بي إم العملاقة السريعة في معالجة البطاقات المثقبة، منشغلاً بموضوعات خفية سرية مثل مؤشرات الأسعار في أمريكا اللاتينية أَو نيوزيلندا، استشعر بنفسه قوة هائلة كأنما يحرّك جبالاً. ولو كانت ييل تدرس علم الكومبيوتر كمادة رئيسة لانتسب رايفست إلىٰ ذلك الفرع فوراً. ولكنَّه مضى بعد تخرجه من ييل بإجازة في الرياضيات ليتابع دراساته العليا بستانفورد، وفي قسم علم الكومبيوتر الذي تأسّس منذ أربع سنوات.

ولقد أمضى رايفست جُلَّ وقته في مختبر الذكاء الاصطناعي المتطور في ستانفورد، مشاركاً في مشروع شبه خيالي، لإنتاج إنسان آلي متحرّك. وكان الغرض من هذا المشروع هو تركُ هذا الوحش الإلكتروني ليجول في موقف السيارات دون تدخّل بشري؛ وكان هذا من المشاريع المبالغة بالتفاؤل، والتي دأب على دراستها العاملون في المختبر في عقد الستينات من القرن الماضي. ولقد استمتع الرجل بالعمل هناك أشد الاستمتاع، وذهبت بلبه فكرة إكساب الكومبيوتر «ذكاء». لكن المشكلات التي ينطوي عليها جعل الإِنسان الآلي

منضبطاً، اضطرته للتركيز على معضلات هندسية محضة، بينما لم يكن يشاء الابتعاد كثيراً عن المجال النظري. ووجد نفسه يزداد نزوعاً إِلىٰ فهم رياضيات الحساب ذاته. ولم يكن مرشده يومذاك الشيخ في مختبر الذكاء الاصطناعي جون مكارثي، وإنما دون كنوث، الحجة في الخوارزميات في ستانفورد. غير أن هدف رايفست كان دائماً تطبيق النظريات في مجال عملي.

يقول رايفست: «إن «الذكاء الاصطناعي موضوع ملتبس ـ ومن العسير معرفة ما تقوم به في هذا المجال، كما أنه يصعب الجزم إن كنت أنجزت عملك على الوجه الصحيح. ولكنك تستطيع بالنظرية أن تأتي بنموذج (موديل) وتقول هاكم ما أريد عمله وهاكم الحل لتنفيذه». وليس هناك كاستخدام الرياضيات الرائعة، في حل معضلة من المعضلات. ففي عالم الرياضيات، أنت قادر، ليس على انتقاء سهم من الفكر من كنانتك ثم إصابة الثور وسط جبهته، وبين عينيه لتنال منه مقتلاً وحسب، وإنما لديك، ما يشبه الحَكم الذي لا يأتيه الباطل من جانب ـ هو برهانك على صحة قضيتك ـ فيصدر رنيناً ليشير إِلىٰ صواب ما أتيت به. وهكذا بينما كان رايفست يستمتع بكتابة برمجيات الذكاء الاصطناعي كانت أطروحته تتناول خوارزميات استعادة قاعدة البيانات وأساليب البحث. وواضح في هذا تأثير كنوث. ولما نال شهادة الدكتوراه ذهب رايفست ليمضي عاماً في العمل في المعهد الوطني للبحوث المعلوماتية والأتمتة INRIA، خارج باريس، منصرفاً للبحث في قضايا نظرية أخرى.

في خريف 1974 قَبِل عرضاً بالعمل في منصب أستاذ مساعد في معهد ماساتشوسيتس. وكانت تلك وظيفة مثالية، لأنَّها تتيح له متابعة اهتماماته النظرية، في قسم يسمح له بحرية العمل في مشكلات البرمجة أيضاً. وكان رايفست قد تزوج بعيد تخرجه من جامعة ييل. وبدا وهو في السابعة والعشرين مهيأً لبدء حياة حافلة بالإنتاج، ومع ذلك هادئة، كأكاديمي في إحدى أفضل المؤسَّسات العلمية في الولايات المتّحدة. وكان له أن يشرف من نافذة مكتبه

في الطابق الثامن من بناية تيك سكوير الشبيهة بالعلبة في كمبردج، ويرى مشهد غروب الشمس الرائع فوق مباني الجامعة ويزيد من تأثيرها، ما تنفثه المصانع في منطقة بوسطن من الدخان. وكان إذا تأمّل هذا المشهد، عاد ليتابع البحث في خوارزمياته.

ولقد ظل رايفست طوال شهر كانون الأول/ ديسمبر 1976 وفصل الشتاء بعده، يعالج الخوارزميات التي عرضها ديفي وهيلمان، في بحثهما «المثير للاهتمام». بل نستطيع القول أنّه انشغل بالصِّيغ «الناقصة» في البيان الكريبتولوجي ذاك. ففي حين أن ذينك الباحثين في ستانفورد قد عرضا، فعلاً، معالم خطة رياضية لطريقة جديدة لتبادل الرسائل السرّيّة ـ وتوقيعها رقمياً بحيث يتثبت المستلم من صدورها عن صاحبها ـ فإنَّهما قصرا تقصيراً جلياً في موضوع تطبيق تلك الخطة عملياً. فقد كانت طريقة تبادل المفتاح التي عرضها ديفي وهيلمان تقوم على أنه يشكّل طرفان مفتاحاً مشتركاً بينهما، ولكن لم يكن ثمة طريق جلية تبين إمكانية أن تشمل التواقيع. (وفي هذا قصر حل الحقيبة لميركل والذي لم يكن قد نشر بعد، أيضاً). وكان ديفي وهيلمان قد قلبا مختلف الطرق على وجوهها علَّ المرء يخرج بطريقة عملية يتمكن بها كل فرد من امتلاك زوج المفاتيح الخاصة به، أحدهما مفتاح عام والآخر مفتاح سري. ولكن هذا لن يزيد عن كونه مجرد رأي، بدون الرافعة الرياضية السليمة. فكل الأمر هنا معلّق على إيجاد الدوال (التوابع) الوحيدة الاتجاه لقوة مناسبة. وقد يتساءل المرء هل هناك حقاً مجموعة منها، ويمكن الاعتماد عليها، كرافعة لمنظومة كريبتوجرافية شعبية؟ مجموعة من التوابع سليمة، تجعل النظام الذي يقوم عليها منيعاً، أمام كل المتنصتين ومفككي الشّيفرة، حتى ذوي المصلحة بمعرفة ما يجري بين الطرفين والمزودين بالكومبيوتر الفائقة السرعة، والخبرة المعمَّقة بالكريبتوجرافيا، وإن كانوا أنفسهم على قدر من العبقرية؟

لقد استولت تلك الأسئلة على رايفست، وباتت الإجابة عنها شغله

الشاغل. ومع أن الجانب الرياضي من هذا البحث كان ينطوي في حد ذاته على قدر عظيم من التشويق لرايفست، إلاَّ أن ما زاد في جانب الإثارة منه أن العملية حافلة برمتها بمتعة التلهف، بما تنطوي عليه من إمكانية الإتيان بحل يطلق نوعاً من التجارة جديداً كل الجدّة ـ فعاليات اقتصادية تجري عبر شبكات الكومبيوتر. ورأى رايفست يومئذ أن في هذا أمراً هاماً، فشرع بالتبشير بالتحدي المطروح فوراً بين زملائه.

كان ليونارد أدليمان أول ضحايا حملة التحريض التي باشرها رايفست. وكان هذا رياضياً شاباً يوزع وقته كصاحبه، بين مختبر الكومبيوتر وقسم الرياضيات. ويذكر أنه دخل مكتب رايفست في ذلك اليوم من كانون الأول/ ديسمبر، وهو على بعد بضعة اعتاد من مكتبه في تيك سكوير. فسأله رايفست: «هل قرأت هذا البحث؟ إنه يعرض لك كيف تصوغ هذه الرموز السرِّيَّة، إذا شئت أن أبعث إليك برسالة، وكنا نريد أن يبقى الأمر سرياً، بينما هناك شخص يصغي...».

وتساءل أدليمان في سره، فيما كان رايفست يمضي في عرض أسلوب عمل المفتاح العام: «أتراني أهتم بهذا الأمر؟ وكان ليونارد أدليمان على النقيض من صاحبه يعيد النظرية. فلطالما كان يشغل فكره بالعلماء جاوس وإيولر وفيرما... عمالقة القرون الماضية الذين اكتشفوا الحقيقة الرياضية العقول الصافية الذين لا يحفلون بما قد تأتي به التطبيقات العمليَّة لنظرياتهم. لقد كان هؤلاء العباقرة بمثابة الآلة عند ادلمان، ولم يكن هو ليتوق إلىٰ أمر أقل من التجول في حلبات العقل المحض ذاته التي كانوا يجولون فيها. أما هذا الحديث عن الكريبتوجرافيا، الذي أثار حماس رايفست، ذلك المبلغ العظيم من الإثارة، فقد بدا لأدليمان أشبه بمسألة تتصل بأسلوب صناعة سيارة أفضل أَو شيء من هذا القبيل. ولم يكن ذلك من المصارعات الفكرية التي كان عبقري من أرباب الرياضيات مثل كارل فريدريش جاوس يرمي بنفسه إليها. وهكذا ظل

أدليمان ينتظر بصبر حتى ينتهي رايفست من حديثه، ثم قال: «إن ما عرضته لأمر مثير للاهتمام كثيراً، يا رون». وانتقل بعدئذ إِلىٰ الحديث في موضوع آخر.

وكان حظ رايفست أفضل مع وافد جديد لقسم الكومبيوتر في معهد ماساتشوسيتس للتكنولوجيا. ففي ذلك الشهر، كان قد حل في المعهد آدي شامير، وهو إسرائيلي ذو وجه نحيل، وشخصية ذكية وطريفة، أستاذاً زائراً في مختبر علم الكومبيوتر، ووجد شامير نفسه هناك في غمرة العمل. ومع أنَّه كان رياضياً من مستوى عالمي، إِلاَّ أنَّه بدا بحاجة لتعلم الكثير في موضوع الخوارزميات. ولذلك كانت مفاجأة له غير سارة، حين تلقى قبل عدة أسابيع، رسالة من رايفست يطلب منه الاستعداد «لمناقشة موضوعات منهاج الخوارزمية المتقدمة الذي ستقوم بتدريسه في فصل الربيع من العام الدراسي». فشعر يومئذ بالانقباض يستولي عليه، إذ حسبه من تدريس الخوارزمية خبراً سيئاً، فما بالك بمنهاج في الخوارزميات العليا؟ ولطلاب يحضرون لشهادة الدكتوراه أيضاً؟ ولحسن الحظ، كان شامير دارساً سريع الاستيعاب. فما أن حل في تيك سكوير حتى شق طريقه إِلىٰ المكتبة. وأخذ يتفحص رفوف الكتب التي تتناول الموضوع؛ وما أن مضى أسبوعان حتى كان قد ألمّ بكل ما يحتاج إِلىٰ معرفته عن الخوارزميات. وفيما كان الرجل ماضياً في القراءة وترميم معرفته، أطل عليه زميله الجديد، رون رايفست، في مكتبه، وعمل على ضمه إِلىٰ الجهد المبذول في تنفيذ كريبتوجرافيا المفتاح العام.

ما أن اطلع شامير على البحث الذي وضعه ديفي وهيلمان حتى وافق رايفست الرأي في أهميته. ولم يكن مصدر أهميته أنَّه جاء بجديد من وجهة النظر الرياضية. فكان رأيه أنَّك إن أخذت شخصاً ذا خبرة بنظرية الأعداد، وحاولت شرح فكرة ديفي وهيلمان أمامه لاستوعبها في دقيقتين بلا زيادة أوَ

نقصان. فكانت الجدية في الأمر، منهج فريق ستانفورد في التقاط ما لم يكن له علاقة بالكريبتوجرافيا في أي وقت من الماضي على الإطلاق، ثم تطبيقه فجأة في حقل جديد. وهكذا سرعان ما أصبح شامير شريكاً لرايفست في البحث عن المزيج المثالي للتوابع (الدوال) الوحيدة الاتجاه.

ولقد توطدت العلاقة بين رايفست وشامير مع مرور الوقت وباتا صديقين، وشكلا مع أدليمان فريقاً ثلاثياً. فقد انضم رايفست، من قبيل التنازل في البداية، إلىٰ البحث الخوارزمي. ويقول أدليمان: «كنا من أعمار متقاربة نوعاً ما، ندرس جميعاً ذات المنهج، واستلطفنا بعضنا البعض، وهكذا لم نعد مجرّد زملاء وشركاء في العمل وحسب، بل غدونا نمضي الوقت معاً ونتردَّد على الأماكن معاً». كان أدلمان وشامير عازبين، وغدت حياة رايفست الذي ينزع إلىٰ ملازمة البيت أكثر من الآخرين بمثابة المرفأ الذي يلجآن إليه، إن أثناء العمل وإن في بيته في بيلمونت، وهو عبارة عن شقة دافئة مفتوحة على فسحة لطيفة. (كان أدليمان يقيم في ناحية أرلنجتون، بينما شامير في كامبردج). ومع مضي الأسابيع بدأ الشبان الثلاثة، المتجاورون في المكاتب في الطابق الثامن من تيك سكوير، ينكبّون على عملهم بكل جد ونشاط.

كان رايفست أشد الجماعة، تركيزاً على الموضوع الذي يتناوله. فمع أنه كان يدرس بعض المواد في تلك الفترة، إلاَّ أنَّه لم يبتعد بجهوده العقلية عن الكريبتوجرافيا. ويقول أدليمان في وصف صاحبه: «كان رون يتقن عمله حق الإتقان، ومهما يكن هذا العمل. فلو عزم على بناء سفن طائرة، مثلاً، فإني أراهن بكل ما لدي أنَّه سيكون في غضون خمس سنوات، أعظم من يشيد سفينة طائرة». وكذلك كان شأن شامير، شخصية مثابرة، ويصفه أدليمان بقوله: «إن آدي أشبه بالأسد فكرياً؛ حسبك أن ترمي أمامه بقطعة من اللحم فإذا به ينقض عليها ويشرع في التهامها».

أما أدليمان فكان أقرب إلىٰ النقيض من زميليه. فمن بين الثلاثة كان أشبه

في مظهره وسلوكه بالمختص بالرياضيات الحالم، ويمثّل نمط الفتى ذي الشعر الأشعث الطويل، الذي يغدو ضحية بريئة للبطلة السخيفة الحمقاء في ملهاة جنونية. (وإن تبينا في نهاية الفيلم أن للفتى بعض النزوات الشيطانية في أعماقه). وقد اعتاد رايفست وشامير أن يعرضا، مرّة أَو اثنتين في كل أسبوع، مشروعاً على أدليمان، رجل النظرية بين الجماعة، فيأخذ في دراسته ويكتشف ما فيه من ثغرات وهفوات، فيرسل بالرياضيين الآخرين إلىٰ السبورة، ليعيدا النظر في ما تفتق عنه ذهنهما، ويعملا على تقويم ما بدا فيه من اعوجاج أَو اضطراب وإصلاح ثغراته. وكان هذا بالنسبة لأدليمان أمراً يسيراً كضرب الذباب، وليس أكثر من ذلك لأعمال الفكر. ولقد ظل يرى حتى بعد مضي أسابيع في العمل، أن المشروع كله دون قدراته فعلاً، لأنه أكثر صلة بالعالم الواقعي مما ينبغي. وأدرك يومئذ أن رفيقيه وجدا النواحي التطبيقيَّة في العمل أمراً يزيد البحث جاذبية. ولكن لم يكن لذلك أي تأثير عن أدليمان. فقد كان الرجل يعشق الرياضيات لأن ما فيها من الجمال يتجاوز الاهتمامات الأرضية.

في البداية كانت كل خطة يأتي بها شامير ورايفست، تسقط متهاوية أمام هجوم أدليمان. وكان في ذلك شيء من الإحباط. ويقول رايفست في وصف حال الجماعة يومذاك: «كنا نتوسل في اختباراتنا بالكثير من المناهج، ومنها ما كان قد عرضه ديفي وهيلمان. ولم نكن راضين عن المناهج التي اعتمدناها في اختباراتنا». ولقد بلغ بهم اليأس في مرحلة من مراحل العمل، ما جعلهم يتساءلون إن كان ثمة حل للمشكلة المعروضة على الإطلاق. وساورهم اعتقاد يومئذ أن ما يبدو من انطلاقة عند ديفي وهيلمان، هو قنبلة صلبة لن يقيض لها أن تنفجر. وهكذا كان أن استبدلت الجماعة عدتها بأخرى، وشرعوا بمهاجمة المعضلة من النهاية المقابلة، محاولين تقديم برهان على استحالة تنفيذ المفتاح العام. ويعلق رايفست على ذلك الوضع بقوله: «ولم نستطع المضي بعيداً في هذا الاتجاه».

في شباط/ فبراير ذهب الرياضيّون الثلاثة من معهد ماساتشوسيتس للتكنولوجيا إِلىٰ منتجع كلينجتون للتزلج بولاية فيرمونت لقضاء العطلة هناك. وكانت تلك، بالتأكيد، عطلة عمل. فحتى حينما كان علماء الكومبيوتر الثلاثة يحاولون تعلم التزلج، كانت عقولهم منشغلة بالمعضلة. ذلك أن الأمر كان بالنسبة لشامير، وأكثر من ذلك لرايفست، مسألة بيولوجية تحفّز على العمل؛ أما أدليمان فقد ذهب معهما على سبيل المسايرة: كانت المعضلة شاغلنا في الحديث، ونحن نصعد بسيارتنا إِلىٰ المنتجع، أَو نتحلّق حول النار، فماذا كان أمامي سوى الانخراط في الحديث والنقاش». كان الحديث ينقطع طبعاً أثناء الاندفاع على المنحدر أثناء التزلج، إذ ما كان بوسعهم متابعة النقاش في تلك اللحظات، ولكنَّهم كانوا بدلاً من ذلك يديرون الموضوع في عقولهم. ويستذكر شامير، بين الجد والمزاح، أنَّهم اتفقوا يومئذ على عادة أن يجري كل منهم يومياً نصف ساعة متزلجاً على المنحدر، ويطلع بخطة مبتكرة للمفتاح العام. ثم يكون على الآخرين تحطيم هذا الحل. وما كاد يحل اليوم الثاني، حتى كان دور الإسرائيلي في تجربة التزلج لأول مرة، وزيّن له الفكر في ما بعد تلك التجربة بقوله: «كنت أتزلج في طريقي على المنحدر، وإذا بخاطر يداهمني، ويمتثل في عقلي فجأة أعجب تصور للمفتاح العام. ولقد بلغ بي الانفعال مبلغاً جعلني أترك زلاجتي، بينما أنا مندفع نحو أسفل المنحدر. ثم تركت عصا الدفع. وفجأة وجدتني وقد خلا ذهني من كل أثر لمخطط الحل. وما زال آدي شامير لا يدري إِلىٰ اليوم إن كان هناك مخطط كريبتو ألمعي، لم يقيض له من يكتشفه بعد أن تُرك مهجوراً في كلينجتون.

كانت المصاعب التي واجهت، هؤلاء الرياضيين الثلاثة، بمعنى من المعاني، متوقعة. فما الذي يحمل أي إنسان على الاعتقاد أنه بوسع ثلاثة من الأساتذة المساعدين في علم الكمبيوتر، الشباب، أن يخرجوا بنظام كريبتو سليم، ناهيك، عن مخطط متين يتيح للناس، لأول مرة في التاريخ، التخاطب

مع بعضهم البعض في سرية تامة دون الاضطرار لوضع ترتيبات خاصة مسبقاً؟ إن العقل السليم يقر بأنه لا يمكن أن يأتي بمثل هذا المخطط إلاً شخص ضليع بهذا المجال. ولو كان لديك آلة سحرية قادرة على قياس المعرفة الكريبتوجرافية لعلمت أن كل ما اجتمع لهؤلاء الثلاثة من الخبرة في معهد ماساتشوسيتس لن يسمح لهم بأن يحركوا شعرة واحدة من محلها.

غير أن هذا الجهل كان أهم ما في عدتهم. ويقول شامير مستذكراً: «كنا محظوظين جداً. فلو كنا نلم بشيء في الكريبتوجرافيا ونعلم ما هي المتتابعات التفاضليَّة، ولوسيفر، ومعيار تشفير البيانات، لضللنا الطريق، وأخذنا بالتوسّع في هذه الأفكار، ولتوسلنا بها في كريبتوجرافيا المفتاح العام. ولكننا كنا هواة حديثي العهد بالموضوع ـ ولم تكن لنا دراية بالكريبتوجرافيا. وكنا بالنتيجة نستقصي الأفكار التي ندرسها في الجامعة».

كانت هذه الأفكار جعبة رياضية تحتوي على كافة الاحتمالات، بدءاً من الجبر الخطي حتى مجموعات المعادلات. ولقد خبروها جميعاً. وكان هؤلاء العلماء يلتقون على العموم في مكتب رايفست، وإذا حلوا فيه أخذوا يخربشون معادلاتهم على السبورة. ومن المألوف عندئذ أن يطلع أحدهم بفكرة فيمضون بعض الوقت في تدبّرها بفكرهم، ولربما وقعوا حينئذ على مثلب فيها أَو خطأ. ويقول رايفست في وصف حالهم في تلك الأيام: أحياناً كنت أنا من يقوم بنقد مشروعي، أَو ربما كان آدي ينقد مشروعه أَو لربما عمدت أنا إِلىٰ نقد مشروعه. أما المشاريع الأكثر تعقيداً فكانت من نصيب أدليمان الذي أخذ يبدي موهبة باهرة في جلاء الخيوط التي تكشف عن خطة معينة، بالرغم من عزوفه في البداية عن العناية بالموضوع أصلاً.

وفي النهاية، وقع الثلاثة على نظام بدا لهم واعداً. وكان هذا المشروع هو الثاني والثلاثين بين المشاريع الواعدة. ولقد وجده أدليمان الأدعى للاهتمام من كل مشروع قبله. فانكب الرجل على دراسته ليلة كاملة قبل أن يتمكّن من

تفكيكه وقد قال فيه أنه «اقتضى القيام ببحث معمّق حتى تغلّب عليه، وليس مجرد الملاحظة [كما كان الحال مع المشاريع الأخرى]»، على حد تعبيره، واكتشف في نفسه مشاعر مختلفة حول إمكانية نجاحه. ولكن بات الآن مدمناً لهذا البحث. (نشر بعض الباحثين دراسة بعد عدة سنوات وطرحوا فيها خطة مماثلة، لم ينالوا منها سوى الحرج، حين اكتشفوا من جديد خطة الهجوم 32 لأدليمان).

ولكن الحلول التي خرج بها الثلاثة أخذت تتجه عند هذه المرحلة، إلىٰ التوسّل بفكرة واعدة للدالة الوحيدة الاتجاه، وهي التحليل إلىٰ العوامل. وجدير بالذكر، أن كنوث كان قد أشار على ديفي وهيلمان بالأخذ بهذه الفكرة، إلاّ أن هذين الباحثين الستانفورديين لم يتبّعا هذا الرأي؛ وبمحض الصدفة كان رايفست قد أخذ بهذا الحدس الذي قال به أستاذه القديم.

وعود على بدء: التحليل إلىٰ العوامل هو مسألة رياضيَّة ترتبط بالأعداد الأولية. والعدد الأولي ليس بالعدد الذي نتوصَّل إليه بضرب عددين، طبعاً (إلاّ أن يكون العدد الأولي ذاته مضروباً بالرقم واحد). أما إذا قمت بضرب عددين أوليين كبيرين فلسوف تحصل على عدد أضخم، ولكنه ليس عدداً أولياً. ولتحليل ذلك العدد إلىٰ عوامله عليك أن تعكس العملية بطريقة ما، محدداً البذرتين الاثنتين اللتين أنتجتاه. وهذه المسألة الصعبة عرفت منذ ما قبل الميلاد ببضع سنين، حين ابتكر إيراتوستثنيس الإسكندري عملية رياضيَّة تدعى «الغربلة» في محاولة لتحقيق هذا الحل.

وكان الناس في ذلك الزمن يعتبرون تحليل العوامل، مسألة تعادل محاولة معرفة: إن كان العدد أولياً أم لا. وبعد حوالي ألف ومئتي عام، قام فيبوناكي بتطوير الطريقة قليلاً، لكنه لم يعرض طريقة يمكن بها تفكيك الناتج إلىٰ العددين الأوليين اللذين نتج عنهما. وعندما تبين جاوس في عام 1801 أن تحليل العوامل واكتشاف أولية الأعداد، مسألتان مختلفتان عن بعضهما كل

الاختلاف، وصف العملية الأولى، تحليل العوامل، بتحدٍ مزعج لكنّه هام:

تعرف مسألة التمييز بين الأعداد الأولية والأعداد المركبة وتحليلها إِلىٰ عواملها الأولية، بأنّها إحدى أهم مسائل الحساب وأشدّها نفعاً من الناحية العملية. . . . إن كرامة العلم ذاته تقتضي البحث عن كل وسيلة لحل مسألة هي على هذا القدر من الجمال والشهرة.

إِلاّ أن جاوس لم يأت بأي حل ناجع لمسألة التحليل إِلىٰ العوامل قط، ، ولا أتى به شخص آخر أيضاً، علماً بأنّه لم يكن هناك دليل على استحالة وجود حل لها. مع أنّها لم تكن قضية الساعة في السبعينات من القرن العشرين. وفي هذا يقول رايفست: «لم يكن التحليل إِلىٰ العوامل بالمسألة التي ينشغل فيها الناس يومذاك. فالبحوث في موضوعها كانت قليلة ومتباعدة من حيث توقيت النشر».

ومع ذلك فإن الرياضيين الثلاثة من معهد ماساتشوسيتس باتوا يزدادون ميلاً، وهم يتابعون تجاربهم ومختلف تنويعات الخطط، لتنفيذ التصور الذي طلع به ديفي وهيلمان، لاستخدام تحليل العوامل في منظومتهم.

في 3 نيسان/ أبريل 1977 أقامت طالبة تحضر لشهادة الدكتوراه تدعى آني بروس احتفالاً بعيد الفصح اليهودي في بيتها. وكان من بين الحاضرين رايفست وشامير وأدليمان. وقد شغل هؤلاء لعدة ساعات عن الأفكار التي تدور حول الصِّيغ الرياضيَّة وتحليل العوامل لاستعادة قصة هروب الشعب اليهودي من مصر. وكالمعهود في مثل هذه الاحتفالات تجرع القوم مقادير كبيرة من الشراب. وكان الوقت قد أشرف على منتصف الليل، حين عاد رايفست وزوجه إِلىٰ البيت. وبينما كانت جيل رايفست تتهيأ لدخول الفراش تمدّد رون على الأريكة وراح يفكّر في المعضلة التي استغرقته ورفيقيه طوال الشهور الماضية. وكانت هذه عادة دأب عليها، فيتمدد على الأريكة، وعيناه مغمضتان، وكأنما هو مستغرق في نوم عميق. وكان من عادته أحياناً، أن يهب منتصباً على قدميه،

ويشرع في تقليب صفحات كتاب ما، دون أن يقرأ فيه شيئاً، وإنما يعيد صياغة الأعداد. وكان لديه كومبيوتر تابع في بيته، إلاً أنه لم يشغله في تلك الليلة، ويقول أنه كان «منشغلاً بالتفكير وحسب».

كان الوحي قد داهمه في تلك الليلة ـ صاعقة من الإدراك نزلت به، تعرف بلحظة إيوريكا (وجدتها)، وها هو ذا قد وجد خطة! كانت شبيهة ببعض محاولاتهم الأخيرة من حيث استخدام نظرية الأعداد وتحليل العوامل. أما هذه فكانت أكثر بساطة، وأكثر أناقة. جهد لأن يتمالك نفسه، محاذراً الاستسلام للانفعال ـ أفلم يستطع شامير وأدليمان نسف الكثير من عروضه من قبل ـ وراح يدّون بعض الملاحظات. ولكنه سمح لنفسه بأن ينعم ببعض التباسط مع زوجه، فأخبرها عندئذ بأنّه جاء بفكرة قد تنجح في حل المعضلة. ولعل انشغاله بفكرته ليلتئذ، قد صرف ذهنه عن الاتصال بصاحبيه ليخبرهما بما صادفه. غير أن أدليمان يصر مع ذلك على أنّه تلقّى منه مكالمة بعيد منتصف الليل.

قال رايفست معلناً: «لدي فكرة جديدة». ومضى يستفيض في شرحها.

كانت فكرة رايفست في جوهرها تقوم على تجريد مسألة تحليل العوامل، حتى تبقى على عناصرها الأساسية تقريباً. ويكون تكوين المفتاح العام وفق هذه الفكرة بضرب عددين أولين كبيرين (ما يزيد عن 100 رقم عشري) مختارين عشوائياً. وهذا أمر سهل. ثم تأتي خطوة سهلة أخرى (إذا كان لديك كومبيوتر): اختر عدداً كبيراً آخر، بعد، رقماً ذا خصائص محددة يسهل حسابها. وهذا ما سوف يعرف بمفتاح التشفير. والمفتاح العام الكامل، يتألّف من مفتاح التشفير وناتج هذين العددين الأوليين.

وقد قدم رايفست عندئذ صيغة بسيطة يمكن لشخص يرغب في تشفير رسالة ما، استخدام المفتاح العام في تنفيذ العملية. فيمكن عندئذ تحويل الرسالة العادية إلىٰ رسالة مشفَّرة، تحولت بشكل عميق إلىٰ معادلة تتضمَّن ذلك الناتج الكبير. وأخيراً كفل رايفست، معتمداً على خوارزمية مستقاة من عمل

إقليديس العظيم، تحقيق مفتاح فكّ الشّيفرة، وهو مفتاح لا يمكن حسابه إِلاً باستخدام عددين أوليين. وباستخدام مفتاح فك الشّيفرة يستطيع المرء تحويل النص المشفّر إِلىٰ رسالة عادية.

وإذا ما نظرنا إِلىٰ الأمر بطريقة أخرى، وجدنا الرسالة الأصلية مرتبطة ارتباطاً وثيقاً، وهي في سبيلها لأن تصبح نصاً مشفراً، بناتج العددين الأوليين. وما جعل المعلومات المتضمنة في النص العادي الواضح مبهمة غير مفهومة، إنما هو تحول رياضي أصاب ذلك الناتج الكبير، وهو تحوّل لا يمكن عكسه إِلاً إذا كنت تعرف هذين العددين. وعندئذ يصبح كل شيء واضحاً لك.

إن قدراً من رياضيات مفتاح فك الشّيفرة ـ وهو يؤدي وظيفة المفتاح الخاص في هذا النِّظام مستمد من أعمال الرياضي الأسطوري ليونهارد إيولر، الذي طلع في عام 1763 بمعادلة تتصل ببقايا الأعداد المتحققة بعد قسمة الأعداد التامّة. ولكن هذه الفكرة التي كانت أهميتها محصورة بالرياضيَّات النظريَّة وحسب، غدت موضع تطبيق، بعد مئتي سنة منذ أن طلع بها صاحبها السويسري، في آليات الشّيفرة في عالم الواقع.

ولقد جاءت الخطة محقّقة لكل متطلبات ديڤي وهيلمان. وأصبح بوسع المستخدم أن يذيع على العلن مفتاحه العام، لأن العنصر الأساسي فيه نتاج العددين الأوليين وحسب. وإذا ما أراد راصد تفكيك رسالة اعترضها وكانت مشفَّرة بمفتاح عام، فلسوف يجد المعلومات أمامه غير ذات جدوى. إذا أراد إيجاد مفتاح لفك الشّيفرة لا بدّ له أن يجد الأعداد الأولية الألية. ولكن كيف السبيل إِلىٰ ذلك؟ إن ذلك لا يتحقَّق إِلاً بتحليل العوامل، وهذا ما عجز عنه حتى جاوس العظيم. وكانت هذه روعة الدالة الوحيدة الاتجاه: سهلة إن كنت تسير في الاتجاه الصحيح، ممتنعة أَو تكاد، إن أتيتها من الطرف الخطأ. وإذا ما استخدم المرء في هذا النِّظام أعداداً أولية كبيرة كالتي كان رايفست يوصي بها، فإن تحليل عوامل ذلك الناتج يقتضي الانقطاع للعمل مع كومبيوترات ضخمة

طيلة الشتاء الطويل، وعدة بلايين من شتاءات أخرى. وإذن فالخطة تظل منعتها مكفولة ما دام تحليل العوامل المكونة فيها عصياً.

ولكن الخطة لم تكن مقصورة على التشفير وحسب. فإذا استخدمت مفتاح فك الشّيفرة (الخاص) لتعمية رقم، فإن الناتج المشوش ذاك يمكن توضيحه، باستخدام مفتاح التشفير وناتج الأَعداد الأولية، المفتاح العام. ولما كان صاحب المفتاح الخاص المحفوظ في حرز أمين قادر على تنفيذ فكّ الشّيفرة، فإن هذه العمليّة كفيلة بتأكيد مصدر الرسالة على وجه الدقة. وإذن فما راود مخيلة ديفي وهيلمان في البدء يبدو الآن حقيقة واقعة: صيغة ثابتة لبصمات رقمية، وهي المساعد على نشوء أنواع جديدة من التبادلات التجارية، ووسيلة لإرساء الثقة على شبكة إِلكترونية.

لقد بدت تلك الصيغ رائعة لأدليمان. فكان ذلك نظاماً دون سواه، مما كانوا يعالجونه من الأنظمة المتعِبة من قبل. وكان هناك آخرون استخدموا برامج معقَّدة نسبياً، تقوم على عمليات الضرب والقسمة والجمع. سوى أن رايفست كان قد أصاب الهدف في الصميم. قال أدليمان لصاحبه يومذاك: «أعتقد يا رون أن هذا هو الحل المطلوب، وأظن أن البرنامج سوف ينجح». ولكن أدليمان شأنه شأن صاحبه لم يتسرَّع فيهلّل للاكتشاف الجديد. فكم من فورة حماس أصابت قوماً في الليل، فإذا كان الفجر تبخرت، حين نظر المرء إِلىٰ أفكاره في ضوء الشمس الساطعة.

غير أن شيئاً من ذلك لم يحدث، إذ لم ينل شيء في صباح اليوم التالي، من روعة الحل الذي أتى به رايفست. فلما التأم شمل الثلاثة كعادتهم في المكتب في تيك سكوير، وجدنا رايفست يقدِّم لصاحبيه مخطوطة ناجزة تنتظر الأمر بالطباعة. وكان عليها تواقيع أدليمان ورايفست وشامير. ويستذكر أدليمان وقائع ذلك الحدث بقوله: «نظرت إِلىٰ هذه المخطوطة فإذا فيها تفصيل لما قاله

في الليلة السابقة». ولقد شعر يومئذ أن ما أمامه هو حل طلع به رايفست. وليس هو من جاء به.

قال أدليمان لرايفست: «اشطب اسمي. فهذا عملك أنت».

ولقد أصر رايفست على أن هذا هو مشروع جماعي، ومساهمات شامير وأدليمان كانت حاسمة في إنجازه، والبرنامج كان النقطة الأخيرة في عملية متطورة. وكان الرأي عند رايفست أنه ما داموا ثلاثتهم قد ركبوا هذا المركب سوية، فعليهم التناوب في تسييره بالتجديف والملاحة بحثاً عن أرض جديدة. فإن صادف أن كان هو ـ رايفست ـ أول من نزل من القارب، إلاّ أنّهم جديرون جميعاً بالمشاركة في نيل الثناء على هذا الكشف. ومع ذلك فقد ظل أدليمان على معارضته. فقد يكون شامير في رأيه قد ساهم في تصورات المشروع، إلاّ أن أدليمان لم يفعل جلّ الوقت سوى وخز بالونات الاختبار بالدبابيس. وما كان ليسمح لرأي أن يزحزحه عن موقفه برفض التنويه بمشاركته في المشروع.

ولقد ألحّ رايفست على أدليمان أن يعيد النظر في موقفه خلال الليل، وليقرر بعدئذ في اليوم التالي. ويقول أدليمان في وصف ما جرى بعدئذ: «وهكذا عدت إلىٰ المنزل وشرعت أنظر في الأمر». فقد كان الرجل، بعد كل أمر، رجل منطق ولئن كان يشعر في أعماقه بأنه لا يستحق مشاركة صاحبيه في فضل الاكتشاف إلاّ أنه أدرك أن ظهور اسمه على أية مطبوعة قد يفيده كأكاديمي طموح حين يسعى لاحتلال كرسي في الجامعة. ولم يكن تفكيك مشروع صاحبيه «البرنامج 32» بالأمر الذي يستخفّ به. فماذا لو أنّه لم يكن ضمن الحلقة لنقد البرنامج، ومضى رايفست وشامير في نشر بحث أساسه الثغرات، فلا ريب بأنّهما كانا سيبدوان أشبه بالحمقى، إذا ما طلع أحد المتخرجين الناشئة المبتذلين وعرى لهما مشروعهما. وإذن ففي ضوء هذا الاعتبار كان الرجل قد قدّم مشاركة، فعلام مجادلة رون في رأيه؟ وذهب به الفكر إلىٰ أن هذا بحث،

ليس مقدراً له أن يغري بالاطلاع عليه، إلاّ أهل الاختصاص. ويستذكر أدليمان تلك اللحظات: «لقد اعتقدت يومئذ أن هذا من أضعف البحوث التي يظهر عليها اسمي». وهكذا كان أن وافق أدليمان على الإبقاء على اسمه على البحث، شرط أن يكون الأخير. وفي تلك الأثناء كان شامير وأدليمان قد اتفقا في الرأي على أن يكون اسم رايفست المتقدم. ومن هنا كان اسم الخوارزمية «ر ـ 1» ار اس إيه RSA، نسبة إلىٰ الحرف الأول من اسم كل من المؤلفين الثلاثة.

وسرعان ما أحال رايفست، اعتماداً على مساهمة زميليه، المسودة الأصلية إلىٰ مذكرة فنية، من مختبر معهد ماساتشوسيتس لعلوم الكومبيوتر، تحمل رقم 82: «منهج لتنفيذ هويات رقمية ومفتاح عام». وكان ذلك يوم 4 نيسان/ أبريل 1977. ومع أن أدليمان ربما كان ما يزال يقلّل من أهمية البحث من الناحية الرياضية فإن نظرة سريعة إلىٰ الكلمات والعبارات الأساسيّة» المعروضة لأغراض الفهرسة، تبين أن هذا كان في أقل تقدير جهداً غير مألوف يصدر لثلاثة قوارض أرقام، من معهد ماساتشوسيتس. والحقيقة، أن الكلمات قدمت مخططاً مذهلاً لجمعية مترامية الأطراف، لم يشع أمرها طوال عشرين عاماً:

. . . توقيعات رقمية، مفتاح شيفرة عام، الخصوصية، التثبّت من الهوية، الأمن، تحليل العوامل، عدد أولي، بريد إلكتروني، نقل الرسائل، نقل الودائع المالية إلكترونياً، كريبتوجرافيا.

ولقد جاءت أولى الكلمات في البحث بضجة وصخب يذكّر بالعمل الذي طلع به ديفي وهيلمان وأطلق هذا المشروع، معلنة أن «عهداً جديداً من البريد الإلكتروني لن يطول حتى يسهل؛ وعلينا عندئذ أن نكفل صيانة عاملين من مكونات نظام «البريد الورقي» الراهن. وهذان العاملان هما: الإبقاء على خصوصية الرسائل والتوقيع. وقد قطع المؤلفون وعداً، بالكشف عن وسيلة

يمكن بواسطتها استخدام هاتين السمتين، اللتين طالما اعتُبرتا خاصية الرسالة المدونة، في العصر القادم القائم على تشابك الاتّصالات.

ولقد برز في البحث غلبة الطرفة. فبدلاً من الصيغة المألوفة في تعيين مستلم الرسالة والمرسل بالحرفين الهجائيين مثلاً: ألف للمرسل وباء للمستلم، عمد رايفست إلىٰ تشخيص الطرفين بإضفاء صفة الجنس والهوية عليهما. وهكذا طلع البحث عن الخوارزمية «رسا» بشخصية «بوب» المتخيل الذي يريد توجيه رسالة إِلىٰ أليس. ولئن يبدو هذا أمراً غير ذي بال للقارئ، فإن هذين الاسمين باتا في الواقع معتمدين في البحوث اللاحقة، التي تعرض التطورات في كتابة الشّيفرة والشخصيات التي كانت تخلو منها البحوث الرياضية في الماضي فأصبحت تتسع لتشمل المتنصتين مثل إيف، ومجموعة من الشخصيات المشاركة مثل كارول وترينت وديف ووايري. ولقد غدا ظهور هذه الشخصيات رمزاً للشخصيَّة المتمرّدة للجماعة الجديدة من المعنيين بكتابة الشّيفرة المستقلين والذين يعملون خارج إطار الحكومة وقيودها وأسرارها.

وبالرغم من لغة الثقة والاعتداد التي كان هؤلاء ينطقون بها، فإن رايفست لم يكن واثقاً من مبلغ دلالة هذا الاكتشاف: «لم يكن واضحاً لي يومذاك إن كان هذا [المخطط]، مقدر له السقوط في غضون بضعة شهور. ولم يكن واضحاً كذلك إن كانت هناك طرق أفضل [للخروج بخوارزمية ناجعة]». ومع ذلك فقد أخذ يعد للنشر في المجلات العلمية، طامحاً لأن يُنشر في مجلة جمعية الآلات الحاسبة. كوميونيكيشنز أف. ذي. إيه. أم. سي. التي كان يساهم في هيئة تحريرها. وقد أرسل نسخاً من بحثه ليطلع عليها زملاؤه. وكان من بين هؤلاء دون كنوث. كذلك بعث بنسخة منه إِلىٰ هويتفيلد ديفي ومارتين هيلمان، وهذا أول اتّصال بكاتبي مقال «اتجاهات جديدة في الكريبتوجرافيا»، الذي أقام عمله على أساس المنهج الذي وضعاه، (وتلك صلة أعلن عنها صراحة في بحثه). (وقد أوضح رايفست فيما بعد، أنّه ليس بالأمر الغريب بين

الباحثين، أن تعمد مجموعة من الأكاديميين إِلىٰ الإفادة من عمل سابق دون إعلام الباحثين الأصليين، حتى بلوغ نتيجة البحث الراهن).

وكان ثمة أمور تحتاج للتذليل، قبل تقديم البحث إِلىٰ مجلة، ومنها تحديد حال التحليل إِلىٰ العوامل على وجه الدقّة ـ فالنظام يعتمد، على صعوبة استخلاص عددين أوليين كبيرين من العدد الناتج عن ضربهما. وكان أن اتصل عبر مارتي هيلمان بريتش شرويبل، هاوي الكومبيوتر في معهد ماساتشوسيتس القديم الذي سبق أن قام ديفي بزيارته أثناء مغامرة البحث التي خاضها وقطع فيها الولايات المتحدة. (ومن المفارقة أن شرويبل كان متشائماً في نظرته إِلىٰ إمكانية قيام منظومات شيفرة، تعتمد على الدالة الوحيدة الاتجاه). وكان شرويبل بين القلّة على هذه الأرض، الذين ما زالوا يولون تحليل العوامل عميق تفكيرهم.

كان شرويبل مستعداً آنذاك لطرح الشك عنه في أمر الدوال الوحيدة الاتجاه ومتلهفاً للمشاركة. فبعد قراءة شرويبل ما قدمه دون كنوث على أنه أفضل صيغة لتحليل العوامل، وضع تحليلاً له موائماً للحال، مدركاً أعمق الإدراك لمبلغ تعقيد المسألة: وأساس ذلك: أنّك كيفما تدبرتها وجدت العمل المطلوب، تحليل عوامله، أضخم كثيراً من الجهد المبذول في حساب عملية الضرب الأولية. وهو يقول في عرض الأمر: «أعتقد أن هذه هي أول مرة درس فيها شخص مبلغ الصعوبة في التحليل إِلىٰ العوامل». وقد أعجب شرويبل بالبحث حول الخوارزمية «رسا» وأرسل إِلىٰ مؤلفيه ببعض الاقتراحات، ومنها تحليل للزمن الذي تستغرقه أسرع طريقة لتحليل العوامل (دراسة غير منشورة لشرويبل ذاته) في تفكيك المفاتيح. النتيجة: زمن طويل إذا كانت منظومة التشفير متينة.

ولقد أرسل رايفست نسخة من البحث أيضاً إِلىٰ مارتين جاردنر صاحب زاوية Mathmatical Recreation في مجلة العلوم الأمريكية Scientific American، لأنّه، على حدّ تعبيره، «دأب على تكريس تلك الأعمدة للكتابة عن الأرقام

الكبيرة، وهو أبداً يبحث عن الأَعداد الأولية». وكان لجاردنر جمهور يدأب على متابعة عموده من هواة الحساب ومن الرياضيين الجادين؛ ولم يكن بالأمر غير المألوف أن تصبح إحدى موضوعاته الشهرية موضوع اهتمام عالم الرياضيات.

وفي 10 نيسان/ أبريل 1977، أي بعد أقل من أسبوع واحد من الكشف الذي أتى به رايفست، كتب إليه جاردنر: «إن مشروعك [الإنشاء] توقيع رقمي لساحر فعلاً. والفكرة التي يقوم عليها جديدة عليَّ، وأعتقد أنَّها جديرة بكتابة عمود ممتع جداً للقرّاء». ثم دعا رايفست لأن يقوم بعرض فكرته بذاته.

ولقد استبد الحماس برايفست، فأسرع إِلىٰ منزل جاردنر في هدسون بنيويورك. وكان جاردنر رجلاً راقياً، سامي الصفات من المدرسة القديمة وعلى قدر من الخبث. وقد قام الكاتب بعرض بعض الخدع بورق اللعب لزائره، وما زال رايفست حتى بعد مضي سنوات، يعجب كيف استطاع تنفيذها. ولما انتهى العرض السحري، طلب جاردنر إِلىٰ رايفست أن يعرض عليه طريقة نظام الخوارزمية «رسا». ثم جاء دور رايفست ليعرض سحره. فقام بتوليد مفتاح عام، من 129 رقماً استخدمها في تشفير رسالة سرِّيَّة. فإذا نجح نظامه كما يتوقع، لم يكن هناك في العالم من يستطيع قراءة الرسالة، عدا شخصين. وكان هذان الإستثناءان: إما شخص [الاستثناء الأول] لديه كومبيوتر قوي قادر على تفيك الرسالة بهجوم شامل ويتمتع بقدر عظيم من الوقت: فإذا كان جهاز الكومبيوتر PDP-10 الذي تبلغ قيمته مليون دولار، فإن العمل سوف يستغرق منه حوالي كوادريليون من السنين (كان هذا التقدير، وقد عرضه رايفست بناء على سوء تفسير على ما يظهر لتحليل شرويبل لعامل الزمن، خطأ من جانبه؛ وما قصد الرجل قوله أن تفكيك الشيفرة حسابياً، سوف يستغرق مئات الملايين من السنين. ومهما يكن فإن هذا جهد لا يقدر عليه البشر الفانون). أما الاستثناء الثاني فهو طبعاً الشخص الذي يحمل المفتاح الشخصي المماثِل لذاك المفتاح

العام ذي الـ 129 رقماً. وهذا الشخص يملك تفكيك شيفرة الرسالة في غضون ثوان.

ولكن ماذا لو قصر نظام «رسا» عن العمل كما كان الوعد؟ في هذه الحالة، سيكون الأمل معقوداً على ظهور قارئ ألمعي همّام ليأتي بالحل الصائب. ولسوف ينال هذا الشخص مبلغ 100 دولار، هو الجائزة التي وعد بها رايفست وشامير وأدليمان، ثم تقام جنازة سريعة لهذا النِّظام ويطوى ذكره كأداة لا تجدي نفعاً في صون حرية البشر والتثبت من حقيقة هوياتهم.

ولقد ظهر عمود جاردنر في عدد آب/ أغسطس 1977 من مجلة العلوم الأمريكية، وكان موشى كله بالثناء على الإنجاز الذي حققه العلماء الثلاثة في معهد ماساتشوسيتس. وقد توقع جاردنر، بأن تضع الكشوفات العلمية التي طلع بها ديفي وهيلمان، ثم الخوارزمية «رسا» نهاية عهد بكامله من تفكيك الشّيفرة، إذ كتب يصف هذه الفتوحات بأنَّها «ثورية ولربما دفعت عما قريب كل الشيفرات وطرق تفكيكها حتى الآن إلىٰ زوايا النسيان». وأضاف الكاتب أننا سوف ندخل من الآن فصاعداً عصراً ذهبياً من الإتِّصالات الإلكترونية المأمونة، حيث تكون الرسائل جميعها مصانة، لا يقدر على قراءتها حتى الراسخون في تحليل الشّيفرة. وفي الواقع، استغل جاردنر المناسبة، ليعلن بطلان ما ذهب إليه [الشاعر والناقد الأمريكي] إدجار آلان بو، من أن «عبقرية الإنسان لا تستطيع أن تأتي بشيفرة يعجز العقل البشري عن حلها». ففي رأي جاردنر أن عبقرية «غرباء» ستانفورد ومعهد ماساتشوسيتس قد أتت بهذه الشّيفرة الخارقة العصية على التفكيك. ولكن الكاتب، وإن أثار الاكتشاف حماسه، اعترف بأنَّه يتمنَّى بأن يجعل الواقع المستجد من التجسّس والتجسّس المضاد في كتابه الشيفرة، أمراً من مخلفات الماضي: «هناك في أرجاء العالم كله رجال ونساء، وبعضهم من العباقرة، كرَّسوا حياتهم للتفوق في علم كتابة الشّيفرة الحديثة... وهؤلاء القوم يقفون أمام أبواب سحرية على وشك أن تُفتح لهم، ولعلها تخفيهم تماماً عن العيون».

ثم أنهى جاردنر العمود برسالة قام بتشفيرها رايفست، متوسلاً بنظام «رسا» RSA ومستخدماً مفتاحاً مكوناً من 129 رقماً، داعياً من يشاء ليجرب حظه ومهارته وقدراته في تحليل الشّيفرة وتفكيك الرسالة. وقد تضمن العمود دعوة القرّاء للمبادرة إِلىٰ تحليل الشّيفرة، أَو طلب مزيد من المعلومات، بإرسال مغلف يحمل الطوابع البريديَّة اللازمة إِلىٰ معهد ماساتشوسيتس، لتزويدهم بنسخة من البحث.

كان الأساتذة الثلاثة بعيدين عن المعهد وهم يمضون عطلة الصيف، ولكن السكرتيرات في مبنى المختبرات في تيك سكوير يشهدن على ما كان للعمود الذي كتبه جاردنر من تأثير، إذ ما أن ظهر هذا المقال حتى انهالت الرسائل متدفقة بالآلاف على المكتب. فلما عاد شامير من إجازته في ألاسكا إِلىٰ كمبردج اصطدم بما هو أشبه بجبال الثلج من الحقائب المختنقة بالمغلفات البريديَّة وقد ضاقت بها غرفة مكتبه، وهو وسطها يتعثّر بينها.

كانت هذه أولى البشائر على الحماس الذي أوقده جاردنر، وكان ذلك أول إعلان عام عن الحركة التي بدأت بالسعي المتفرد والثوري، الذي بادر إليه هويت ديفي، وبدا وكأنما أطلق كل مشاعر الإحباط الحبيسة، لكل من استحوذ عليه فترة من الزمن، فن الشّيفرة المحاط بالأسرار، إنما ليسمو بذلك الاهتمام في مكان آخر، نظراً لأن كل ما هو حسن في عالم من الشّيفرة محصور في البقعة خلف السياج مثلث الأطوار، أَو مثيلها في دول العالم. ولقد كانت قراءة ما كتبه جاردنر لما بدا أنه نقطة تحول في هذا التاريخ للكريبتوجرافيا، وليس بما يتعلّق بالأدوات وحسب، إنما أولئك الذين ابتدعوها أيضاً ـ أشبه بالشمس إذ تطلع بعد عقود من الكآبة والضباب.

كان لين أدليمان قد شاهد أول دليل على هذا في شهر آب/ أغسطس، وهو يستطلع إحدى المكتبات في بيركلي. فبينما كان ينتظر دوره لتسديد ثمن مشترياته من المكتبة، طرق سمعه حديث بين أحد الموظفين وزبون اشترى

مجلة العلوم الأمريكية Scientific American، حيث سأل هذا الزبون: «هل رأيت ما كُتب هنا عن طريقة جديدة للشيفرة؟».

فأجاب الموظف: «نعم لقد قرأت عنها! أليست أمراً خارقاً؟» ولم يتمالك أدليمان نفسه، فتدخل في الحديث، قائلاً: «هذه طريقة نحن ابتدعناها»، وتابع فعرَّف عن نفسه بأنّه أحد الأساتذة الثلاثة بمعهد ماساتشوسيتس الذين ورد ذكرهم في عمود جاردنر. ولما أدرك مشتري المجلة أن أدليمان جاد في قوله قدَّم له نسخة المجلة قائلاً: «هل تتفضَّل بتوقيعك على المقال».

وهكذا بوصفه أداة في تحرير الكريبتوجرافيا من قيودها، وجد أدليمان نفسه فجأة شخصية مرموقة، فيُطلب منه توقيعه كما لو كان من نجوم السينما المشاهير مثل توم كروز. وذلك امتياز لم يتحقَّق مثله حتى لعالم الرياضيات العظيم فيرما!

وبعد، ماذا عن أولئك الذين يقفون عند تلك الأبواب السرِّيَّة التي تحدّث عنها جاردنر، أي واضعي الشّيفرة ومفكّكيها، والمحلِّلين، والأشباح التي تختفي يومياً في دوامة الصمت في فورت جورج ميد؟ ثم كيف وجدوا العمل الذي جاء به رايفست وشامير وأدليمان، وطروحات ديڤي وهيلمان؟ كما يمكن للمرء أن يتوقع: مرعباً جداً.

كانت حقبة منتصف السبعينات، فترة عصيبة لوكالة الأَمن القومي. فقد استمرت علاقتها بالكونغرس على مدى السنوات الخمس والعشرين الماضية على منوال واحد، سمته سرعة إصدار التشريعات بما يوافق الوكالة. ودأب المشرعون، بعد جلسات الاستماع التي تُعقد في الغرف السرِّيَّة النظيفة من كل جهاز استماع مدسوس، على الموافقة على كل ما تطلبه «القلعة» من أمور. ولكن الوكالة وجدت نفسها في العامين 1975 و1976، مدار تحقيق لا يعرف الهوادة من لجنة الاستخبارات التي كان يرأسها السيناتور فرانك تشيرتش، حول ما قامت به من أعمال التنصّت على المكالمات الهاتفية. وقد صُدمت

اللجنة إذ وجدت الوكالة تقوم وفق خطة استراتيجية، أُطلق عليها اسم: مشروع شامروك Shamrock (النفل نبتة برسيم مثلثة الأوراق) بأعمال التنصّت على المكالمات الهاتفية على نطاق واسع، بما في ذلك، تلك التي يجريها مواطنون أمريكيون. وكان أشد ما أثار حنق السيناتور تشيرتش الاستخفاف في تأكيد الوكالة على أن أعمال التنصّت كانت تتم دون الحصول على موافقة القضاء. ولما صدر التقرير النهائي كانت الخاتمة التي وضعها تشيرتس أشبه بالوعيد في الكتاب المقدس، بما قد يحصل إن استمرت الوكالة على نهجها دون ضابط أو قيد محذّراً من أن قدراتها على التنصّت والرصد «قد تنقلب في أي وقت ضد الشعب الأمريكي، وعندئذ لن يتمتع أي أمريكي بأي قدر من الحرية الشخصية. . . فالقدرة على رصد كل شخص وكل ما يدور [تعني] أنه لن يكون لأي إنسان. . . مكان يختبئ فيه». ولئن استطاعت وكالة الأَمن القومي تفادي العواقب الخطيرة لهذا «العرض الفاضح» (على حد وصف أحد المسؤولين في الوكالة في مذكرة داخلية) فقد كان له وقع الدواء الذي يعيد المخمور إلىٰ رشده.

ولقد أدرك العقلاء في الوكالة يومئذ أن هذا هو الوقت الذي ينبغي فيه إبداء الخضوع والامتثال. ومع ذلك فقد كان العمل الذي خرج به ديڤي وهيلمان، وما تلاه من متابعات عملية منذرة بما هو أخطر، بمثابة اعتداء على ما تعتبره وكالة الأَمن القومي حقاً لها بموجب الولادة: السيطرة على كتابة الشّيفرة. فهذا أمر لا تملك الوكالة أن تتجاهله أو تغضّ الطرف عنه. ذلك أنّه لو امتلك الناس الوسائل لتشفير رسائلهم الخاصة لوجدوا لأنفسهم الملجأ الذي يختبئون فيه ـ أما أن تكون ثمة وسيلة عامة شائعة للحفاظ على الخصوصية، فذلك أمر ما كان لوكالة معهود إليها بالتنصّت، إلاّ أن تحول دون تحقيقه. ومع أن إدراك مثل هذا التهديد لمهمة الوكالة كان يستغرق طويلاً. في مسالك الجهاز البيروقراطي المعقد في فورت ميد. فقد كان من الجلي أن بعض المسؤولين فيها، أدركوا حقيقة المشكلة. وأساس ذلك أن الوكالة أخذت منذ عام 1975 بالعمل وراء

الكواليس (وهل هناك سوى ذلك؟) لتقييد هذا الحقل الأكاديمي الناشيء.

وكان أن وجهت أولى جهودها نحو المؤسَّسة القومية للعلوم National Science Foundation NSF، وهي وكالة حكومية مستقلّة تهدف إِلىٰ رعاية البحث في كافة نواحي العلم؛ وكان من الشائع جداً أن يعمل الرياضيون وعلماء الكومبيوتر في بحوث ممولة، على الأقل جزئياً، من المنح التي تقدمها هذه المؤسَّسة. (وقد ضمت قائمة المستفيدين من هذه المنح ديڤي وهيلمان والفريق الذي قام بمشروع «رسا»). وفي حزيران/ يونيو 1975 تلقى فرد واينجارتن، المكلف بمتابعة مخصّصات هذه المنح، في المؤسَّسة القومية للعلوم، تحذيراً من أن وكالة الأَمن القومي هي المؤسَّسة الحكومية الوحيدة ذات السلطة لتمويل البحوث في الكتابة بالشّيفرة. وقد جزع واينجارتن، إذ خطر بباله أنه قام بخرق للقانون. وهكذا توقف عن تقديم أي منحة جديدة، حتى تنجلي له الأمور.

وكان ما اكتشفه واينجارتن طريفاً. فعند المطالبة بالوثائق، تبين أنه لا محامي المؤسَّسة القومية للعلوم، ولا وكالة الأَمن القومي ذاتها تمكّنوا من أن يأتوا بأي مبرِّر قانوني يدعم ادعاء الوكالة. وهكذا رأى واينجارتن نفسه حراً، في تجاهل التحذيرات التي بلغته ومتابعة تقديم المنح.

كان مارتي هيلمان من بين الذين يقدِّرون جرأة واينجارتن، فيذكر: «لما طلبت منه وكالة الأَمن القومي ألا يمول برامج الكريبتوجرافيا فهذا حكر على الوكالة وحدها، فإن «فرد» لم يكن شجاعاً وحسب، في تعامله مع الوكالة، بل أثبت كفاءة في ذلك أيضاً. فهو لم يبادرهم بالهجوم والتنديد، وإنما سألهم تزويده بعرض خطي لمطلبهم، ليحمله إِلىٰ محاميه لسؤاله الرأي والمشورة».

ولكن في ذلك الوقت، ظهر البحث الذي وضعه ديڤي وهيلمان. ثم أعقبه الكشف الذي عُرف بخوارزمية «رسا» RSA. فكان أن وضعت هاتان المصادفتان معاً، الأُسس لأسوأ المخاوف لدى وكالة الأَمن القومي، أي ظهور

أنظمة اتِّصالات يتمتع كل امرئ فيها بشيفرة مأمونة. وهكذا لم يكن من قبيل الصدفة المحضة، أن يغادر نائب المدير المساعد لوكالة الأَمن القومي لشؤون أمن الإتصالات سيسيل س. كوري فورت ميد، يوم 20 نيسان/ أبريل 1977، ولم يكن قد مضى إِلاَّ ثلاثة أسابيع أَو أقل، على توزيع رايفست مذكرته الفنية التي تحمل اسم معهد ماساتشوسيتس للتكنولوجيا، إِلىٰ العاصمة للقاء واينجارتن، وبصحبته أحد زملائه. ولقد كرَّر المسؤولان محاولة منع المؤسَّسة العلمية القومية من تقديم منح تتصل بالكتابة بالشّيفرة، متوسلين بما قدماه كتوجيه رئاسي ينيط بـ [وكالة الأَمن القومي] مهمة «السيطرة» على البحوث في هذا المجال. فقام واينجارتن بتذكيرهما بما أثبتته تجربته السابقة من عدم وجود هكذا توجيه. ومع أنَّه وافق على توجيه العروض المتصلة ببحوث كتابة الشيفرة إِلىٰ وكالة الأَمن القومي بحيث يمكن لها تقديم تقييم فنيٍّ عند دراسة المنحة، فقد أصرّ على أن يكون ذلك علناً، وألاّ يتخذ أي قرارٍ خلف ستار الصمت.

ولم تكن هذه بالتسوية التي يسعد بها هذان المسؤولان، وقد بلغ بهما الضيق مبلغاً، جعلهما يلمحان باستخفاف لواينجارتن بأنَّهما «سوف يضطران لاستصدار قانون [من الكونغرس]»، لمنع هكذا بحوث علمية، كما للمرء أن يفهم من مغزى الكلام، ما لم يكن أمثال ديفي وهيلمان ورايفست في العالم، يقبلون بدفن عملهم تحت شارة السرِّيَّة. ولقد كتب كوري فيما بعد، إِلىٰ رئيس واينجارتن، جون باستا، شاكراً تنازلاً لم تقم به المؤسَّسة القومية للعلوم قط، وهو قبول أخذ «الآثار الأمنية» بالاعتبار، عند دراسة طلب المنح. وقد أوضح باستا على نحو لا يقبل الالتباس، أن المؤسَّسة لم تقطع على نفسها مثل هذا الوعد للوكالة.

وفي مذكرة وضعها فرد واينجارتن في ذلك الحين، لخص الرجل وجهات نظره في الدوافع التي تحكم الوكالة:

إن وكالة الأَمن القومي محكومة بقيد البيروقراطية. في الماضي كانت

الاتِّصالات التي تراعى متطلباتها الأمنية الضخمة هي الاتِّصالات العسكرية والدبلوماسية وحسب. أما الآن ومع رواج وظائف الحكومة التطبيقيَّة والاتِّصالات البعيدة Telecommunications، فإن الحاجة للمعالجات الرقمية المأمونة جداً قد بلغت القطاع المدني. وكالة الأَمن القومي قلقة، طبعاً، من احتمال تعريض جوانب من عملها للخطر، بسبب البحوث التي تمسّ الأمن العام. ومع ذلك، واستطراداً لما سبق، فإن هذه الجهة تريد على ما يبدو المحافظة على سيطرتها واحتكار الخبرة في هذا المجال. . .

من الواضح أن إناطة مسؤولية وطنية ضخمة، إذ تشمل بالضرورة مؤسَّسات ضخمة مثل المصارف: وريد الولايات المتّحدة، وكابلات التلفزيون بمؤسَّسة كوكالة الأَمن القومي، أمر لا ينبغي الحسم فيه إلاَّ بعد أشد التمحيص وأدق النقاش على أعلى مستويات الحكم بدلاً من أفراد أمثالي، لاهم بالعير ولا بالنفير.

وكان واضحاً أن وكالة الأَمن القومي، لم تكن في وارد الإذعان والإنسحاب.

وبينما كانت السماء تكفهر فوق الطريق المحيط بالمعهد، كان الأساتذة الثلاثة، وجميعهم منشغلون بكتابة الشيفرة، فرحين مرحين يرون الدنيا مغمورة بنور الشمس. وكانوا يجهلون قطعاً كل ما يمت بصلة، لقوانين التصدير في البلاد، والاتفاقيات التي قد تؤثِّر على انتشار عملهم. ولم يكن لديهم أدنى فكرة عن افتراق العام 1977، حيث كانت سمة نصفه الأول، ما قدموا في مجال كتابة الشّيفرة الإِلكترونية من مساهمة بارزة، بينما اتصف النصف الثاني من ذلك العام، بما بذلته الحكومة من جهود لمنع الناس من معرفة مثل هذا العمل.

في صيف ذلك العام، بلغت مكاتب تحرير مجلة IEEE في نيويورك، رسالة مؤرخة في 7 تموز/ يوليو 1977 موجهة إِلىٰ إي ك جانيت مدير العاملين في هيئة المطبوعات. وقد افتتح الكاتب رسالته بالقول: «قد لاحظت في

الشهور الماضية أن المطبوعات التي تصدر على اختلافها عن IEEE، دأبت على نشر وتصدير مقالات فنية في موضوع التشفير وعلم كتابة الشيفرة، وهو حقل فني تحكمه القوانين الفيدرالية. . .» ثم تلا ذلك مقتطفات بالتفصيل الدقيق لتلك التعليمات، كلاً على حدة، مما يمكن أن يكون قد تم خرقها، ليس في ما نشرته مطبوعات الـ IEEE من مقالات معينة وحسب، وإنما في مختلف ندوات البحث التي قامت المجموعة برعايتها، بما في ذلك الندوة التي عُقدت في رونيبي، بالسويد، حيث عرض هيلمان لأول مرة المفتاح العام. وقد ضمن الكاتب، على سبيل زيادة التوثيق، نسخاً مصورة «عن صفحات قليلة للقانون المقصود» أي حصراً «قانون تجارة السلاح الدولية». وقد قصد بهذه الأنظمة «السيطرة على استيراد وتصدير العدة والعتاد العسكري والخدمات الدفاعية». وفي حين أن أناساً مثل رون رايفست كانوا يفترضون دوماً بأن أعتدة الدفاع، هي دوماً تجهيزات مثل أدوات التفجير النووي، والصواريخ المضادة للطائرات وحاملات الطائرات، إلاَّ أنه تبين أن «أدوات الحرب» هذه مشمولة بقوائم الذخيرة في الولايات المتّحدة «بـ» أجهزة الاستسرار [و] أجهزة شيفرة» وكانت كل التجهيزات والأدوات من المواد المحظور تصديرها، دون إذن خاص من وزارة الخارجية. والأدهى من ذلك أن هذه القيود، لم تكن تقتصر على «الأجهزة الحقيقية وحسب، وإنما كانت تشمل أي «بيانات فنية» تتصل بهذه الأسلحة، وهذه البيانات مقصود بها، تعريفَ، أي معلومات غير سرِّيَّة. . . يمكن الاستفادة منها. . . في تصميم أَو إنتاج. . . أَو تشغيل أي سلاح محظور تصديره. فإذا قمت بنقل هذه المعلومات إلىٰ شخص أجنبي، أَو حتى سمحت له بأن يضع يده/ يدها (على سبيل المجاز) على عدتك، فإنَّك تكون بذلك قد خرقْت القانون ـ وإذن أنت عدو للدولة.

ولاحظ صاحب الرسالة أن مجموعة الـ IEEE تعتزم إقامة ندوة دولية في تشرين أول/ أكتوبر من ذلك العام حول نظرية المعلوماتية في جامعة كورنيل

وتتضمن بحوثاً حول كتابة الشّيفرة. وحذَّر من أن مثل هذه البحوث أَو النشرات تخضع لقيود معينة، وإذا ما أرسلت نسخ عنها إِلىٰ الخارج «فقد يصادف [المسؤول] متاعب، لأنه بموجب قانون تجارة السلاح الدولية يشترط فيه الحصول على ترخيص بالتصدير». وكان المفهوم من هذا أن انتهاك القانون قد يؤدي إِلىٰ تعريض [المسؤول] للغرامة والاعتقال، بل والسجن أيضاً. وفي لهجة متجهمة لحظت الرسالة أنه في مؤتمر رونبي [السويد]، «جرى تجاوز هذه الناحية الرسمية».

كانت الرسالة واضحة جلية: إنكم أيها الأكاديميون المعنيون بالكريبتوجرافيا، تعتقدون بأن أفكاركم تتكون تحت مظلة حماية الحريات الأكاديمية وأن ما تأتون به من صيغ رياضية، من شأن الله وحده، وهو أول من وضعها وسواها... ولكن هذا لا يصدق حين يتصل الأمر بأفكار، وخوارزميات قد تستخدم في تشفير المعلومات. وواضح كما تذهب الرسالة في القول أن IEEE إنما تزود عبر الاستمرار في عقد المؤتمر في جامعة كورنيل أعداء أمتنا بما يعادل العتاد العسكري الثقيل بطريقة غير قانونية. ثم خلص الكاتب إِلىٰ القول: أنه «كعضو في الـ IEEE يتمنى على [مجموعة النشر]، إعادة النظر في هذا الوضع، لأن لتقنيات الأسلحة الحديثة هذه، وهي تنتشر دون رقابة، أثراً يتجاوز الأكاديمي».

وقد حملت الرسالة توقيع شخص يُدعى ج. آ. ماير، عرَّف نفسه بعنوان بيته في بيثيسدا بولاية ماريلاند ورقم عضويته في IEEE (مؤسَّسة مهندسي الكهرباء والإِلكترونيات).

فمن هو هذا الشخص الذي استبد به القلق وحمله على كتابة هذه الرسالة، حماية للمصلحة الوطنية؟ لقد تبيَّن عند البحث أن جوزيف آ. ماير هذا نفسه سبق له أن وضع مقالاً لنشره في مطبوعة تصدرها المؤسَّسة اسمها: «تفاعلات متبادلة في الأنظمة الفضائية والإِلكترونية»؛ وكان ذلك المقال بحثاً

غريباً كل الغرابة، مما حمل المحررين على وضع مقدمة تمهيدية حول طبيعته المثيرة للجدل. وفي هذا البحث الذي حمل العنوان «منظومة مستقبل ومرسل لردع الجريمة» يقترح ربط المجرمين من أصحاب السوابق والذين يخضعون لرقابة الشرطة، ومن هم تحت الكفالة بمنظومة تتألَّف من أجهزة راديو صغيرة: مستقبِلة ومرسِلة، مما يكفل رصد وتحديد مواقع هؤلاء. وذهب ماير إلىٰ القول: أننا نستطيع بمتابعة المشبوهين «إنشاء منظومة رصد وكشف وقيادة وسيطرة إِلكترونية للتخلّص من الجريمة». وجاء في النبذة عن حياة ماير وسيرته الذاتية؛ أنه من مواليد نيوجيرسي 1929، وحائز على شهادة بالرياضيات من جامعة روتجرز، وأمضى سنتين في سلاح الجو في أوائل الخمسينات، وانضم بعد ذلك إِلىٰ وزارة الدفاع، حيث عمل بشكل أساسي في مجال الرياضيات والكومبيوتر، والاتّصالات في الولايات المتّحدة والخارج».

والمراقب، يستطيع إذا ما توفرت له بعض الخبرة، أن يعلم: أن الفرع السري في وزارة الدفاع المقصود، هو هيئة يختصر اسمها في ثلاثة حروف NSA وقلما ظهر في المنشورات سنة 1971. بل الحق أن مجلة العلوم Science أكَّدت الشائعات. بعد ثلاثة أسابيع من ورود رسالة ماير، أن جوزيف آ. ماير يعمل في وكالة الأَمن القومي.

ولقد أثارت رسالة ماير شكوكاً عميقة حول وجود علاقة لوكالة الأَمن القومي بالقضاء علىٰ العمل المستقل في مجال الشّيفرة. وكانت هذه الرسالة قد أُرسلت في ذات اللحظة التي تسلم فيها الفريق البحري بوبي إنمان، إدارة وكالة الأَمن القومي وبدأ بشن الحرب ذاتها التي كان ماير قد أعلنها على الأكاديميين المعنيين بالشّيفرة. غير أنَّه لم يظهر في السنوات اللاحقة، أن ثمة ما يدحض ادعاء ماير (الذي أيَّدته وسط ضجيج وصخب وكالة الأَمن القومي) من أنه تصرّف بمبادرة منه دون إيعاز من إنمان أَو أي شخص آخر في الوكالة، حين قام بكتابة رسالته الشهيرة. (يقول إنمان الآن أنه كان يستمع إِلىٰ عرض «تسليم

المهام» من رئيس الوكالة المنقول لويس اللين، في الوقت الذي كان يكتب فيه ماير رسالته، ولم يتطرق الحديث إِلىٰ الشيفرة، ولو من قبيل الإِشارة). وقد توصلت لجنة المخابرات في مجلس الشيوخ، عند النظر في القضية، سنة 1978، إِلىٰ النتيجة ذاتها، بل إن مارتي هيلمان يرجح الآن أن يكون ماير قد تصرف بمبادرة منه كعنصر غير منضبط. ومن جهة أخرى رفضت وكالة الأمن القومي جهاراً أن تندِّد بالرسالة، كما أكد إنمان للكونغرس فيما بعد، صحة الملاحظات التي أوردها ماير.

ولقد كان لرسالة ماير على كل حال وقع مباشر. فالمؤكد أن منظمي مؤتمر كورنيل أخذوا الرسالة على محمل الجد وافترضوا: إن كان ماير مصيباً في ما قال، ينتهي أمرهم والمتحدثين في مؤتمرهم إِلىٰ الملاحقة، والسجن لمجرد عرض أبحاثهم! غير أنه تبين أن موضوع البيانات التقنية، وتعليمات التصدير قد طرحت في الجمعية قبل عقد من الزمن، وكما رد إي ك جانيت، الشخص الذي تلقى الرسالة، على ماير في رسالة تملق مؤرخة في 20 تموز/ يوليو 1977، فإن «كافة مطبوعات مؤتمر IEEE والمجلات التي تصدرها معفاة من شرط الحصول على شهادة التصدير، بموجب الباب 11 ـ 125 (آ) من بنود تعليمات التصدير». ثم تابع ليشير إِلىٰ ملاحظة وردت في ذلك الباب من أن «مسؤولية الحصول على موافقة الحكومة لنشر أي بيانات تقنية تقع على أي شخص أَو شركة تسعى إِلىٰ نشر هذه البيانات». وبعبارة أخرى، كان جانيت يريد بذلك القول أن هذه ليست مشكلتنا ـ إنها مشكلة أولئك الأعضاء الذين يجرأون على البحث في هذا الحقل. ثم أعرب عن امتنانه لماير «للفت انتباهنا إِلىٰ هذه القضية ذات الأهمية»، ووعد بلفت «انتباه الأطراف ذات الاهتمام». ولقد قام جانيت فعلاً بوضع مذكرة للدكتور نارينداي دويفيدي، مدير النشاطات التقنية في المنظمة، وأشار عليه بأن تقوم الـ IEEE بلفت «انتباه الباحثين إِلىٰ قواعد اللعبة».

في 20 آب/ أغسطس وجّه دويفيدي رسالة إِلىٰ الباحثين في ست مؤسسات. لافتاً أنظارهم إِلىٰ أن «عضواً زميلاً معيناً وطيب النوايا قد استرعى انتباهنا إِلىٰ احتمال قيام كتاب بانتهاك تعليمات قانون التصدير. . .

ويبدو أن على مؤسَّسة مهندسي الكهرباء والإِلكترونيات والجماعات التي تنتسب إليها ومنظماتها ومجالسها، والأفراد (ومستخدميهم) توخي الحيطة والحذر». ثم قدم دويفيدي بعض النصائح للجيل الجديد من الباحثين في مجال الكريبتوجرافيا، فذكر أن عليهم توجيه بحوثهم إِلىٰ دائرة الذخيرة بوزارة الخارجية بواشنطن العاصمة، لنيل الموافقة عليها.

إن ما ذهب إليه دويفيدي يتفق أشد الاتفاق مع الأماني التي عبَّر عنها ج. ا. ماير. ولكن المشكلة هي أن الباحث إن سلم وزارة الخارجية ورقة بحثه فإنه في الواقع يتنازل عن سيطرته للحكومة. أما بما يخص الباحثين الثلاثة في جامعة ماساتشوسيتس فإنَّهم سيجدون أمامهم، كما قالت مجلة Science، «نظام رقابة ترصد به وكالة الأَمن القومي الأبحاث التي تجريها، مجموعة نظرية المعلوماتية في معهد ماساتشوسيتس للتكنولوجيا».

كان مارتي هيلمان أحد الذين تلقوا رسالة دويفيدي. وقد هرع يوم تلقاها ليعرضها على رون رايفست وكان يمضي عطلة الصيف من ذلك العام في زيراكس بارك في بالو آلتو على مقربة من جامعة ستانفورد: «وكانت تلك أول مرة أُدرك فيها أن في عملنا ما قد يثير الحساسيَّات»، فلما عاد إِلىٰ المعهد أسرع الرجل تحت تأثير القلق لاستشارة محامي المؤسَّسة.

كان رايفست مهتماً، طبعاً، بالآثار القانونيَّة لإرسال المذكرة الفنية رقم 82 إِلىٰ من يطلبها دون أن يتكبّد أي كلفة سوى الغلاف الذي يحمل اسم الطالب وطوابع بقيمة 35 سنت في إطار «مسابقة» تجريها مجلة «العلوم الأمريكية». وكانت الأسئلة التي شغلت خاطره يومئذ: هل في توزيع ورقة الـ «رسا» على قرّاء المجلة مخالفة قانونية؟ هل يمكن أن يخضع معهد ماساتشوسيتس

للتكنولوجيا للمساءلة القانونية؟ هل يمكن أن ينتهي رايفست وشرويبل إلىٰ السجن؟ وماذا عن شامير؟ إن الرجل أجنبي لا يحمل حتى الجنسية الأمريكية! هل يمكن توريط معهد ماساتشوسيتس في دعوى، لتوزيع بحث هو أحد واضعيه؟

يقول رايفست: «كانت الطلبات للحصول على ورقتنا، تتوارد علينا من كافة أرجاء العالم. وكان بعضها يأتينا من حكومات أجنبية. وكنت يومئذ في حيرة من أمري، فلا أدري كيف ينبغي علينا التصرّف. فأنت حين تتلقى هذه الرسالة المزعجة المنذرة بشر مستطير من وكالة الأَمن القومي، تجنح إلىٰ المحافظة والتأني وترغب في التحقق منها». ولذلك صار الرجل نهباً للخواطر من كل جانب حتى أنه درس احتمال أن يكون بعض ما يرد من البلدان الأجنبية في طلب المذكرة مدسوساً للإيقاع به بتهمة مخالفة تعليمات التصدير، وليجعلوا منه عبرة للرياضيين الذين يتورطون في وطء عتبة وكالات التجسّس المحرمة.

ولقد جاء الرد سريعاً من إدارة المعهد: لا ترسل هذه المطبوعات حتى نجد حلاً لهذه الورطة. على أنه يذكر لرؤساء الجامعة حرصهم على ترسيخ مبادئ الحرية الأكاديمية، فقد أخذوا يعملون يومئذ ما وسعهم لتعبيد الطريق أمام توزيع المذكرة الفنية هذه. فبالرغم من طول عهد المعهد بالعمل مع وكالات الأَمن القومي في أبحاث سرِّيَّة ذات مستوى عال فإن المهمة التي عهدت إليها لم تكن يسيرة. فالتعامل في هذه المرة مع وكالة الأَمن القومي، وبات بعض المسؤولين فيها، على الأقل، في ذعر، وهم يواجهون تحدياً صريحاً لاحتكارهم الشيفرة. غير أنَّهم يجدون أمامهم هذه المرة، خصوصاً ذوي نظرة واضحة، ويؤمنون بأنَّه يجب عدم المجازفة بالحرية الفكرية، بدعوى الحفاظ على الأمن القومي التي لا سند لها في الواقع. وإذن، فلا بد في هذا العصر الجديد في البحث الأكاديمي من وضع قواعد جديدة، ولا بد من اتخاذ

القرارات الكبرى منذ البداية. واعتقد الباحثون في المعهد أنه سيكون من الصعب بعد تأسيس السوابق إحداث التغييرات بصورة جذرية.

وفي ستانفورد وجدنا مارتي هيلمان أيضاً يسارع إلىٰ طلب المشورة من المحامين المتعاقدين مع الجامعة. وفي 7 تشرين أول/ أكتوبر أكّد له محام من هؤلاء، يدعى جون ج. شفارتز: «ليس ثمة في رأينا مأخذ قانوني في نشر نتائج البحث الذي تتحدث عنه». لكن هناك خطر من أن يخطئ المحامون التقدير، وأن يكون ج. آ. ماير يعكس توجهات الحكومة الاتحادية؛ فإذا كانت هذه هي الحال يكون هيلمان عرضة للملاحقة القانونية بسبب توزيع ورقة البحث الذي قام به. فتعهد شفارتز بأن تقوم الجامعة في هذه الحالة بالدفاع عنه. ثم أضاف: «ومع ذلك، فإن هناك احتمالاً قائماً، بأن تُغرَّم شخصياً أَو تتعرَّض للسجن، إذا كسبت الحكومة الدعوى، إن حصلت».

وفي النهاية عُقد مؤتمر جامعة كورنيل ـ وهو موضوع رسالة ماير ـ كما كان مقدراً له، وعُرضت خلاله الموضوعات عينها التي قال ماير أنها تنطوي على انتهاك لأنظمة التصدير وتشكّل تهديداً للأمن القومي. وقد ظهر يومذاك أن الجامعيين يتمتعون بشجاعة أكثر من مؤسَّسة مهندسي الكهرباء والإلكترونيات، التي كانت قد حثتهم على عرض بحوثهم على الحكومة قبل عرضها. بل أن هيلمان تطوع لقراءة بحثين لاثنين من طلابه في الدراسات العليا، حين خشيا أن يصبحا موضوع مساءلة من الحكومة، وهما بعد في مطلع حياتهما المهنية. وقد صرح هيلمان لصحيفة نيويورك تايمز، وهو يعرض موقفه في هذه المبادرة بقوله: «كنت متعاقداً مع [جامعة] ستانفورد، يومذاك، ولو شاءت وكالة الأَمن القومي أن تعرضنا للمحاكمة فإن ستانفورد كانت ستؤازرني. أما الطالب الذي ما زال في أوائل عهده ويطمح إلىٰ بدء الحياة العملية، فسيجد البحث عن عمل مضنياً والتهديد بدعوى تستمر ثلاث سنوات مسلط كالسيف فوق رأسه».

كذلك شارك رالف ميركل في إحدى الجلسات. أما هويت ديفي الذي لم

يكن اسمه مدرجاً بين المتحدثين في المؤتمر، فقد خرج عن البرنامج الموضوع ليتحدث في جلسة غير رسمية على هامش المؤتمر. ويقول أن «اللقاء كان يسيراً لم تتخلّله المتاعب، وعبّرت عن رأيـي بأنه ينبغي تجاهل رسالة ماير».

وبينما كانت الأمور تجري على هذا النحو، كان محامو المعهد ما يزالون يخوضون المشادات مع وكالة الأَمن القومي حول قانونية شحن المذكرة الفنية 82 في 7000 مغلف أرسلها الراغبون بأسمائهم وملصق عليها الطوابع في مكتب شامير لترسل إِلىٰ مكتب البريد. وكان الأكاديميون قد أشاروا إِلىٰ وجود فقرة في لائحة أنظمة التصدير توفر لهم الحصانة من المسؤولية، وهي النص صراحة، على استثناء «المواد المطبوعة، حصراً من المواد المحظورة. فماذا كان رد «القلعة» على هذه الفقرة؟

يقول شامير مستذكراً: «كان من العسير، كما هو العهد بوكالة الأَمن القومي، الحصول على إجابة تامة منها. وكان يتضح باطراد، أن وكالة الأَمن القومي عاجزة عن تقديم مستند قانوني يبرِّر تصرفاتها. وهكذا كان أن أجاز المعهد للأساتذة متابعة العمل في بحوثهم. وفي كانون أول/ 1977، أي بعد نصف عام من نشر عمود جاردنر ومع تدفق الطلبات، دعا أصحاب الخوارزمية «رسا» RSA طلاب الدراسات العليا في المعهد إِلىٰ وجبة بيتزا وحفلة تعبئة مغلفات، وجرى بعدها رميها في صناديق البريد. وهكذا كان أن طبقت شهرة الخوارزمية «رسا» أرجاء العالم أجمع.

كان ينبغي أن ترى وكالة الأَمن القومي، في تداول الآلاف من هذه الأوراق في مختلف أنحاء العالم، فضلاً عن آلاف النسخ المصورة من أوراق ديفي وهيلمان أن الأمور في موضوع الكريبتوجرافيا قد خرجت عن السيطرة، ولم يعد يجدي معها القوانين والمراسيم واتباع أساليب الترهيب لإعادتها إِلىٰ سابق العهد. ومع ذلك، فقد ظلت الوكالة تحاول خلال السنوات القليلة التالية، بحكم العادة أكثر منه كأمل يحدوها، قمع النشاط الفكري في عالم

الكتابة بالشّيفرة، الذي يبدو الآن يزداد اتساعاً وانتشاراً خارج نطاق السياج الثلاثي.

إن المرء إذ يتأمّل في ذلك، يبدو له سلوك المؤسّسة غريباً ومتناقضاً. ولكن، ماذا كان بوسع وكالة الأَمن القومي أن تفعل سوى ذلك؟ فقد يكون لوكالة المخابرات المركزية تاريخ حافل ومقيت من الرشوة ونصب الفخاخ وسوى ذلك من الأساليب، إلاَّ أن الثقافة التي نشأت عليها وكالة الأَمن القومي في فورت ميد كانت ثقافة مختلفة كل الاختلاف عن تلك التي أخذت بها وكالة المخابرات المركزية. فمع أن الوكالة كان لها بالتأكيد نصيب من التجاوزات أحياناً (كما تبيّن وثائق لجنة السيناتور تشيرتش)، فقد بدت المناقب التي تأخذ بها دائماً، وكأنَّها تنظر إِلىٰ البطولة من زوايا المهمات الفكرية الرفيعة من اختزان الإِشارات وابتكار الشيفرات، وتفكيك رموز الشّيفرة. فخلال السنوات التي قطع فيها هويت ديفي البلاد طولاً وعرضاً وهو يسعى إِلىٰ الاستنارة والتوجيه في طلب المعرفة في علم الكتابة بالشّيفرة لم يصدف أن واجه تهديداً ولو مبطناً بالكفّ عن البحث ولا كان هناك أية إشارة إِلىٰ وجود من يترصده في مقهى من مقاهي مدينة بالو ألتو، ويتحين الفرصة ليرميه بسهم مسموم من مظلة مصنوعة خصيصاً لهذا الغرض ليقضي بسمها البطيء. فذلك ليس من الأساليب التي تلجأ إليها وكالة الأَمن القومي.

وهناك، أيضاً، سؤال أشد وجاهة وأحرى بالجواب، هو: «إذا لم يكن من شأن القانون أن يسعف الوكالة في جهودها، فلم تتجشم العناء وتحارب حركة تبحث في الكتابة بالشّيفرة؟» فلا ريب أن هناك استراتيجيين أشد دهاء من بعضهم داخل السياج الثلاثي قد أدركوا أن فورت ميد ربما تفيد، في بعض النواحي على الأقل، من حركة مستقلة تسعى في هذا المجال. ولكن من هو الذي يتمتع بوضع أفضل من وكالة الأَمن القومي، لاستغلال التطورات الثورية في الكتابة السرِّيَّة، وهي التي تتفوّق بالخبرة والمعرفة على أي منافس، إن في القطاع الخاص أو في القطاع العام؟

كانت هذه هي المعضلة التي واجهت الفريق البحري بوبي إنمان، ولم يكن قد مضى على استلامه منصب مدير الوكالة في تموز/ يوليو 1977 سوى أيام. ومع أن إنمان كان قد اكتسب خبرة واسعة في الكريبتوجرافيا بفضل عمله مديراً لمخابرات البحرية، وعمله سنوات قبل ذلك في مخابرات سلاح الإشارة فإن فكرة قيام الغرباء بتحقيق تطورات هامة في الكريبتوجرافيا كانت فكرة جديدة بالنسبة له. فقد كان يؤمن، وهو يوافق في ذلك معظم أقرانه في طائفة المخابرات، وكما يقول الآن، بأن «وكالة الأَمن القومي تحتكر المواهب. فإذا كان ثمة قوم على ذكاء شديد، ويميلون إِلىٰ حل مسائل الكريبتوجرافيا، فالأرجح أن هؤلاء إما يعملون في وكالة الأَمن القومي، أَو في إطار إحدى المجموعات الاستشارية العلمية [ويعملون في إطار السرِّيَّة]». ولقد استفزته هذه الثورة مثل ملاكم غرّ أصابته لكمة لحظة رنين الجرس ببدء العراك، وخاصة منذ ظهور ردود الفعل على رسالة ماير في صحيفتي النيويورك تايمز والواشنطن بوست. ولقد أدرك إنمان على الفور أن هذا لم يكن مجرد خطر جديد يتهدّد وكالته وحسب، بل أن ردود الفعل الجديدة وغير المسبوقة، لها ما يبرِّرها كذلك.

ومع ذلك فقد ظلّت وكالة الأَمن القومي تتصرَّف، خلال الشهور الأولى من تبوء إنمان منصبه، وكأنما القواعد والتوجهات القديمة ظلّت على حالها دون تغيير. وفي تشرين أول/ أكتوبر 1977، تقدم أستاذ في هندسة الكهرباء في جامعة ويسكونسن يدعى جورج دافيدا بطلب منحه براءة اختراع لأداة تستخدم أساليب رياضية في إنتاج شيفرات متدفقة، وعرض مخططات اختراعه دون الاستئناس بأية معلومات سرِّيَّة، كما كانت المنحة المالية المقدَّمة من المؤسَّسة القومية للعلوم غير محكومة بشروط تفرض عليه الحصول على الترخيص لعمله من الدوائر المتصلة بأعمال الدفاع. أما طلب الإجازة ذاته فقد قُدِّم باسم مؤسَّسة أبحاث خريجي الجامعة، امتثالاً لإجراء معمول به ويسمح للجامعة بالاستحواذ على عوائد الاختراع الذي يعود لأحد الأساتذة، وتقوم المؤسَّسة القومية للعلوم

بتمويله. وكان أن تلقى دافيدا بعدئد بتاريخ 28 نيسان/ أبريل 1978 رداً من الحكومة لم يكن يحمل على الموافقة ومنح براءة الاختراع، وإنما كان مرفقاً بورقة تحمل عبارة أمر سري وتفيد بأن وكالة الأَمن القومي تعتبر اختراعه سراً يحظر نشره.

لقد كان الحظر الذي فرضته وكالة الأَمن القومي على تنفيذ الأداة أمراً سيئاً بما يكفي، ولكن الأدهى من ذلك تلك الورطة التي وجد دافيدا نفسه فيها. ذلك أن أمر السرِّيَّة لا يقتصر على الأداة وحدها، وإنما يتجاوزها إِلىٰ المادة الفكرية التي أدَّت إِلىٰ إنتاج هذه الأداة أيضاً. فقد اعتبرت وكالة الأَمن القومي، بالنتيجة، أفكار دافيدا ضرباً من السم، أَو مادة ممنوعة يحظر تداولها. وكان أن وجد دافيدا نفسه وسط معضلة لا يدري كيف يتدبرها، نظراً لأن المواد التي أنتجها كان قد تم توزيعها فعلاً. فهل كان يتوقع منه أن يمتثل فعلاً فيذكر أسماء كافة من اطلعوا على عمله، فيجر زملاءه إِلىٰ عالمه الرهيب من الأفكار التي في كشفها الخطر كل الخطر؟ ولكنه كان من الجهة الأخرى عرضة لدفع غرامة تبلغ عشرة آلاف دولار وقضاء عقوبة السجن سنتين جزاء عدم امتثاله للقانون.

ولكن دافيدا لم يكن وحيداً في هذا المأزق. ففي يوم من أيام نيسان/ أبريل، أصدرت وكالة الأَمن القومي، قراراً بفرض السرِّيَّة على «الهاتف المرحلي» Phasorphone، وهو جهاز يعمل على تشويش الصوت، خرج به مجموعة من العلماء، على رأسهم فني من سياتل في الخامسة والثلاثين من عمره، يدعى كارل نيكولاي. وبعد انتظار استمر خمسة شهور للحصول على إجازة الاختراع لجهاز كان يأمل أن يحقّق صاحبه من ورائه ثروة، جاءه الرد بمنعه من بيع اختراعه، بل وحظر عليه استخدامه أيضاً.

وهكذا أصبح كل من دافيدا ونيكولاي في لغة أجهزة المخابرات «جون دو» [الشخصية المثالية رمز الرجل النزيه الساذج، الذي روج له فرانك كابرا في أفلامه في الأربعينات. هـ. م]. وكانت هاتان حالتين نادرتين نسبياً، كما عرض

لهما جيمس بامفورد في كتابه «قصر الأحاجي» The Puzzle Palace، إذ لم تكن فيها اختراعات مقيتة، منسوخة عن أدوات موجودة وراء السياج الثلاثي، وأصحابها لا يدرون، وإنما هي إبداعات أصيلة تعتبرها الحكومة من طرف واحد أشد خطورة من إجازة تنفيذها.

ولكن ولّت تلك الأيام، كما قُدِّر لوكالة الأَمن القومي أن تعلم فيما بعد، حين كان بوسعها أن تصدر أمراً سرياً فتحظر انتشار عمل من الأعمال، ويكون ذلك القول الذي لا راد له. فكان أن شن دافيدا ونيكولاي رداً على ذلك الأمر، وشرعا في تنظيم حملة واسعة النطاق من كتابة الرسائل المعارضة من شخصيات مرموقة، وإطلاع النواب في الكونغرس على الحقيقة، والاتِّصال بالصحافة حول هذا الموضوع. وكان دافيدا على الخصوص، وهو رجل صغير الحجم مشاكس بطبعه، ولا يميل لتصديق وعود الحكومة الأمريكية، يدوي بصوته في الدفاع عن موقفه. وكان أن التأم بسرعة المسؤولون في الجامعة في اجتماع عاجل، برئاسة رئيسها، لتوجيه كتاب شديد اللهجة إِلىٰ المؤسَّسة القومية للعلوم مطالبين باتخاذ الإجراءات اللازمة للرد على هذا الوضع. كذلك عرض رئيس الجامعة الموضوع أمام وزير التجارة خوانيتا كريبس، التي بدا عليها الانزعاج لتحول مكتب براءات الاختراع بكل بساطة إِلىٰ أداة للرقابة. وفي غضون ذلك، وجّه دافيدا كتاباً شديد اللهجة إِلىٰ مجلة «ساينس» Science قال فيه أن تصرفات وكالة الأَمن القومي إنما كانت ضرباً من المكارثية الأكاديمية.

وكان من نتائج هذه الحملة أن تراجعت وكالة الأَمن القومي عن موقفها، فأصدرت في 13 حزيران/ يونيو من ذلك العام قراراً بإلغاء قرارها السابق. وكان التفسير الذي قدّمه الفريق البحري إنمان أثناء جلسة استماع في الكونغرس فيما بعد «حول السرِّيَّة التي فرضتها الحكومة على الأفكار الخاصَّة» أن القرار الذي اتخذ بحق دافيدا كان خطأ صدر عن موظف من المراتب الوسطى.

كما اتخذ قرار، بعد عدة شهور، بإلغاء القيود المفروضة على براءة الاختراع الخاصة بنيكولاي. ولما كان إنمان ذاته هو الذي ألغى ذلك الأمر السري، فإنه التمس العذر فيما بعد من اللجنة الفرعية التي تنظر في هذه الأمور في الكونغرس، لاتخاذه ذلك القرار تحت تأثير ضغط الأحداث، إذ قال في جلسة الاستماع: «لا بد لك وأنت تتعامل مع قانون سرية الاختراعات من أن تتخذ [أحياناً] قرارات سريعة». ولكنه أصر على أن المشكلة في هذين القرارين لا تكمن في أنَّهما لم يكونا قد صدرا خطأ، وإنما المشكلة في عدم عناية الحكومة كفاية بتطبيقهما». ومع ذلك فإن هذا التعنيف المزدوج قد أوضح أن وكالة الأَمن القومي قد فقدت سيطرتها القديمة في التوسّل بالقانون، لحبس كتابة الشّيفرة في حاويات محكمة الإغلاق، في عهدة الحكومة.

كان إنمان في ذلك الحين، قد توصل إلىٰ قرار بحمل همومه مباشرة إلىٰ المؤسَّسات التي يراوده القلق بشأنها، فشرع في القيام بجولة في مؤسَّسات البحوث، في ما وصفه ديڤيد كاهن بـ «محاولة ناعمة» لكسب تأييدها له. ففي جلسة مشهودة في أحد نوادي جامعة بيركلي، وجد إنمان نفسه وهو يحاول شرح وجهة نظره، يواجه سلسلة متصلة من الأسئلة العدائية. وكانت تلك جلسة وصفها إنمان بـ «حوار الطرشان». ومع ذلك، فقد تخلّل تلك الجلسة لحظات جعلته يعتقد بإمكانية عقد علاقة مفيدة أفضل من هذه التي كانت قائمة. وفي حركة مشهودة تنسب لرئيس وكالة الأَمن القومي اتصل الرجل بمارتي هيلمان وطلب منه اللقاء. وقد قال إنمان في الرجل الذي شارك في اختراع المفتاح العام للشيفرة، وأحد أعتى نقاد معيار تشفير البيانات: «لقد أعجبني [هذا الرجل]. وأعتقد أنه تأثّر إذ وجدني أقود سيارتي، وأنا قادم للقائه، ولذلك كان رده [على طلب بدء حوار حول أسلوب التعامل مع الشّيفرة العلنية] إيجابياً».

حاول إنمان تبديد أقسى الإجراءات التعسفية ضد الباحثين، وكان الكثير

منهم يعتقدون يومذاك، أكثر من أي وقت مضى، بأن وكالة الأَمن القومي، كانت تحاول استدراجهم إِلىٰ داخل السياج الثلاثي، حيث يمكنهم الحد من اكتشافاتهم. وكان من هؤلاء الذين خبروا هذا المنحى عبر تجربتهم الشخصية، لين أدليمان الذي كان ذات يوم الشريك A المعاند في الخوارزمية رسا RSA. فقد ظل أدليمان يتلقى طوال سنوات عديدة منحاً مالية لإجراء أبحاثه من المؤسَّسة القومية للعلوم، والتي كانت تجدد له المنح، دورياً، كل ثلاثة أعوام. ولقد ضمّن العرض الأول الذي قدَّمه بعد مشاركته في الخوارزمية «رسا» قسماً يحدّد بعض العمل وفيه قدر من الرياضيَّات والذي قد يستخدم في كتابة الشّيفرة. وبعد طرح الأسئلة المألوفة في ما يتصل بمثل هذا العرض ـ مثل قضايا الميزانية المخصّصة وما شابه ـ دهش أدليمان حين اتصل به هاتفياً أحد المسؤولين في المؤسَّسة القومية للعلوم يخبره بعزم المؤسَّسة على إجراء مزيد من التعديلات، وخصّ بالذكر أن وكالة الأَمن القومي، سوف تتولى تمويل الجانب الذي يتصل بالكريبتوجرافيا من العمل.

وكان رد أدليمان: «لقد قدمت العرض إِلىٰ المؤسَّسة القومية للعلوم، وليس لوكالة الأَمن القومي؟ أليس كذلك؟».

فصادق المسؤول على قوله، «ولكن الأمر متداخل، على حد قوله، بقضايا تتصل بالوكالة»، ثم أنهى المحادثة عند هذا الحد.

وأصاب أدليمان عندئذ ضيق شديد واشتاط غضباً. كان يدرك أنَّه قد يكون في الأمر مبررات مشروعة تتصل بالأمن القومي للاهتمام ببحوث كتابة الشّيفرة في الجامعات. (إذ ماذا يمكن أن يحدث لو أن أحدهم عرض طريقة لفك شيفرة هامة؟). ولكن هذا كان تجاوزاً، إذ يعني أن وكالة الاستخبارات الأكثر سرِّيَّة في البلاد تمارس تأثيرها على الوكالة الأولى في تمويل البحوث العلمية. ويقول أدليمان في تعليقه: «كان هذا في نظري تهديداً لرسالة الجامعة كلها ومكانتها في المجتمع». ولقد قرَّر الرجل عرض الأمر علناً على الملأ.

فاتصل عندئذ بمراسلة مجلة «ساينس» العلوم جينا كولاتا، وكانت تتابع هذا الصراع وأخبرها بالقصّة.

ولم يمض وقت طويل حتى تلقى أدليمان مكالمة هاتفية، من بوبي إنمان شخصياً. وعرض له مدير وكالة الأَمن القومي أن المسألة كلها كانت ضرباً من سوء التفاهم. ويستذكر أدليمان تلك المكالمة ويقول في وصف إنمان أنه «كان بالغ اللطف». وانتهى الأمر بأن أصبح الباحث، يتلقى المنحة كاملة من المؤسَّسة القومية للعلوم.

كانت تسويات مثل هذه، عند إنمان، أدوات يتوسّل بها لبلوغ ضرب من انفراج العلاقات بعد التأزم مع الأكاديميين، ويكون فيها تلبية متطلبات الأَمن القومي وما يلح عليه الباحثون من حرية الجامعة. وكان يعتقد أنه هو، صاحب الورقة الرابحة الأخيرة، وهي لن تجبر الأكاديميين على اللعب وفق شروطه وحسب، وإنما سوف تؤدي إِلىٰ وقف احتمال تعميم الكتابة بالشّيفرة في العالم. وكانت هذه الورقة الرابحة التي يمسك بها إنمان تكمن في «أنظمة تصدير الأسلحة». وخلاصة ذلك أن إنمان قال في شهادته أمام الكونغرس بعد سنوات من تعيينه في القلعة أنَّه حين حل فيها «لم أكن أدري ما هي هذه الأنظمة، ولكني كنت سريعاً في اكتساب المعرفة».

ولقد أدرك على وجه الخصوص، كما يقول اليوم، «إن المسألة تتوقف، - حين يتعلّق الأمر بالسيطرة على الكريبتوجرافيا، في أواخر القرن العشرين - على «التصدير». وكانت هذه القوانين هي كل العدة التي حالت دون تنفيذ تعميم الكريبتوجرافيا، وشيوعها، ومنعت آثارها التي تبلغ حد الكارثة، وذلك يعادل ذوبان الأَمن القومي. ولقد أدرك إنمان أن القيود المفروضة على ما يمكن تصديره إِلىٰ بلدان العالم وخطر الملاحقة القضائية، في حال انتهاك تلك القوانين، سوف يجبر الناس على التعامل مع وكالة الأَمن القومي، ليس بما هو مسموح لهم بتصديره وحسب، وإنما بما أنتجوا للاستخدام محلياً أيضاً.

ولسوف تصبح هذه الأنظمة الحافظ لجهود الوكالة، لمنع الاتِّصالات الدولية من أن تصبح مشفَّرة.

والمضحك المبكي، أن الجهود التي بذلتها وكالة الأَمن القومي للسيطرة على البحوث الخاصة في الكتابة بالشّيفرة، قد أطلقت سلسلة من الأحداث التي هدَّدت بإفشال هذه الأَنظمة. ولقد كان المستشار العلمي للبيت الأبيض يومذاك رجلاً يدعى فرانك بريس، واسترعى اهتمامه الجدل الذي دار حينذاك حول الكريبتوجرافيا العلنية، فطلب رأي وزارة العدل القانوني، فيما إذا كان في أَنظمة تصدير السلاح، انتهاك لبنود حماية حرية التعبير، التي كفلها التعديل الأول للدستور. وجاء الرد من المحامي العام المساعد، ويدعى جون هاموند، بعد الدراسة والتمحيص وتحليل طريقة صياغة الأَنظمة. وقد اكتشف هارمون أن أَنظمة تجارة الأسلحة لا تشترط طلب الترخيص من تجار السلاح وحسب، بل ومن «كل شخص تقريباً له صلة بالعرض أَو المناقشة، إن هنا وإن في الخارج، وتؤدي إِلىٰ انتقال بيانات تقنية إِلىٰ أجنبي». عروض، محاضرات، ومناقشات؟ حسبكم هذا من التعديل الأول! وفي 11 أيار/ مايو 1978، أعلن مكتب المحامي العام رأيه. وكان فدوياً:

«إن البنود التي تقوم عليها أَنظمة تجارة الأسلحة حالياً هي في رأينا منافية للدستور لأنَّها تحدّ سلفاً من الكشف عن أفكار تتصل بالكريبتوجرافيا ومعلومات توصل إليها علماء ورياضيون يعملون في القطاع الخاص».

وحين بلغ هذا التحليل إنمان، ثارت ثائرته وتهيأ لمحاربته. فأتى بـ«محام فذّ [وعمل على] إقناعه للانضمام، والعمل في وكالة الأَمن القومي لتنفيذ هذا الرأي. وكان من بين الوسائل التي توسّل بها الإدعاء بسابقة قضائية حديثة تجعل رأي هارمون موضع خلاف. غير أن مسؤولاً في وزارة العدل ردَّ هذا التأويل. وقد دحض نائب المدعي العام المساعد لاري هاموند هذا الرأي، بقوله في الرد: «إننا لا نعتقد بأن [السابقة] تحسم قضايا التعديل الأول المعروضة بصورة

القيود المفروضة على تصدير أفكار تتّصل بالكريبتوجرافيا أَو بنفي الحاجة إِلىٰ دراسة أَنظمة تصدير الأسلحة من جديد».

وفي تلك الأثناء كانت وكالة الأَمن القومي تسير على خط حرج. فقد كانت تحاول تهديد الباحثين الذين يقومون بطرح مكتشفاتهم وأفكارهم، بينما هي تعلم حق العلم أن وزارة العدل قد خلصت إِلىٰ أن هذه التهديدات خرق للدستور.

ولقد دار هذا الضجيج بعيداً عن عيون الجمهور، ولا يبدو أن شيئاً من هذا، كان له أثر على النهج الذي اختارته وكالة الأَمن القومي، في تفسير قوانين التصدير. وهكذا فإن هجوم مستشار الفريق البحري هيلمان، وإن كان عاجزاً من الناحية القانونية عن رد البينات التي أتى بها جون هاموند، إلا أنه كان مؤثراً. ذلك أن وزارة العدل حين لم تقم بتعميم حكمها في الأمر كانت متفقة مع وكالة الأَمن القومي، على تجاهل احتمال أن يكون في تنفيذ أنظمة تصدير الأسلحة خرق للائحة الحقوق.

حدث هذا كله خلال عام 1980 في جلسات الاستماع، التي عقدتها اللجنة الفرعية المختصة بالعمليات الحكومية في الكونغرس حول تصنيف الحكومة لسرِّيَّة الأفكار الخاصة». وقد طرح مدير مستشاري اللجنة، تيم انجرام، في سياق هذه الجلسات سؤالاً وجيهاً: «كيف لي أن أعلم، وأنا محام عادي حديث العهد وجد نفسه مشتتاً بعض الشيء في [متاهة] أنظمة تجارة الأسلحة، أنني أواجه الآن قضية سبق لوزارة العدل أن حكمت قبل عامين بعدم قانونيتها؟» فرد أحد المسؤولين في وزارة العدل بأن ذلك الرأي لم يقدم ليفيد منه المواطنون العاديون، وإنما كان مشورة قدمت للوزارة ذاتها.

ولم يكن هذا بالرأي الذي يقبل به انجرام. ولعل انجرام كان يفكر بأمثال رايفست وهيلمان الذين هُدِّدوا بالسجن بسبب عرض أبحاثهم، أَو أقران دافيدا ونيكولاي الذين اصطدموا بالأمر بالتزام السرِّيَّة، أَو الباحثين كلهم مثل أدليمان

الذين يواجهون الآن ضغوطاً أكثر حذقاً، حين طرح سؤالاً آخر:

لديك هذا الرأي الذي يعود إِلىٰ عامين سلفاً، والذي يجد البند [موضوع النقاش] مخالفاً للدستور. وما زال هذا البند ثابتاً لم يطرأ عليه تغيير. فهل هناك ما يلزم الوزارة برفع الأمر في لحظة من اللحظات إِلىٰ الرئيس، وتلفت انتباهه إِلىٰ أن إحدى هيئات السلطة التنفيذيَّة الخاضعة له تقوم بانتهاك الدستور؟

ولقد ظل هذا السؤال دون رد مقنع. وعلى كل حال، كان القلق يساور بوبي إنمان من الحركة الجديدة في الكتابة بالشّيفرة، ويستبد به الضيق لضعف سلطته في مواجهتها. وكان أسوأ ما يخشى أن يكون لتبني الناس للتشفير «تأثير مباشر على قدرة وكالة الأَمن القومي على تقديم معلومات ذات شأن». ولقد بات مقتنعاً يومئذ بحاجة الوكالة لمزيد من السلطة الظاهرة، لتستعيد سيطرتها على الكريبتوجرافيا، وقام في سبيل ذلك بأمر لم يسبقه أحد ممن شغلوا منصبه من قبل، بأن أظهر وكالته إِلىٰ العلن.

كان السبيل الذي اختاره لتقديم نفسه هو مجلة «ساينس»، وكانت أكثر مطبوعة تظهر خلال الأعوام القليلة الماضية جرأة في متابعتها ورصدها الأحداث والتيارات. وكان مجرد منح المجلة حق المقابلة حدثاً في حدّ ذاته. وفي هذا المقال نقل عن ف. آ. و شوارتز الذي كان المستشار الرئيسي في جلسات لجنة السيناتور تشيرتش، قوله: «إنني في حيرة. فقد قيل يوم كنا نعالج موضوع وكالة الأَمن القومي أنه من الخطورة بمكان أن يستجوب [مسؤولي الوكالة] أحد، حتى وإن كان هذا عضواً في مجلس الشيوخ، وفي جلسة مغلقة». ومع ذلك فقد حملت رسالة إنمان أخباراً جديدة أيضاً ـ وتجلى بدعوة مدير وكالة الأَمن القومي الباحثين نهاراً جهاراً للحوار» معه وأعوانه. فقال في هذه المقابلة أن «إحدى الدوافع التي كنت أحملها وأنا أجري أول مقابلة علنية، هي اكتشاف طريقة لإقامة «حوار» جدي لما يمكن عمله [وردم الفجوة] بين فريقين على طرفي نقيض، بين القائلين بـ «الحرص على السرِّيَّة» وأولئك الذين يأخذون

بـ«حرية البحث العلمي». ولكنّه سلم، وهو يكاد أن يلتقط أنفاسه، أن النقاش إن أفلح في ما هو بصدده، واستطاع فرض رقابة على الأبحاث الأكاديمية التي لها صلة بالأمن القومي، سوف ينتهي، «بنقاش بين الإدارة والمجتمع الأكاديمي» (نقاش لن يكون فيه لأساتذة الجامعات المنهكين كبير تأثير في حمل الحكومة على تغيير سياستها الأمنية).

وما هي إلاّ أسابيع قليلة، حتى قام إنمان بخرق أعظم لتقليد السرِّيَّة التي تأخذ بها وكالة الأمن القومي، بأن ألقى خطاباً علنياً دفاعاً عن وكالته. وإن المكان الذي اختاره لإلقاء هذا الخطاب، لم يكن بالنسبة له بالمكان المعادي، وهو اجتماع لجمعية الصناعات الإلكترونية، في كانون الثاني/ يناير 1979، وأعضاؤها يتولون تنفيذ العقود المتصلة بالمشاريع الدفاعية. إن إلقاء إنمان لخطابه، دل على أن بحراً من التغيير، بدأ يضطرب حتى في شخصه. وكانت أولى الكلمات في خطابه بمثابة الاعتراف بذلك، إذ قال: «إن كلمة يلقيها، علناً، مدير تولى حديثاً وكالة الأمن القومي، في موضوع يتصل بمهمة الوكالة، إن لم نقل أنه ذو أبعاد تاريخية، هو على الأقل في حدود معرفتي حدث لا سابق له». والحق أن مجرد النطق باسم الوكالة كان أمراً استثنائياً غير مسبوق.

وها هو ذا إنمان يعترف صراحة بأن العالم قد تغيّر، وليس بخياره. ثم أشار بلهجة الحنين إلىٰ الأيام الخوالي، وحين كانت جماعته «تنعم بنعمة العيش في الظل إلىٰ حدَ ما»، وأفواههم مطبقة، لا تبوح بشيء، عما يعملون ولا تدري به زوجاتهم، بل ولا زملاؤهم في المكتب... أيام كانت وكالة الأمن القومي تؤدي وظائفها الحيوية دون أن تخشى تدقيق الناس في ما تقوم به أو الحوار العلني». ولكن الآن هذا عهد جديد قد بدأ، في ما أسماه بـ «الحوار بين وكالة الأمن القومي وبقية العالم»، حيث حل محل الحياة السعيدة التي أمضتها وكالة الأمن القومي «كلياً في الظل» عهد من «التوترات المعقدة» بين الحكومة

وأولئك الذين ينشدون الحوار مع بعضهم، دون تطفل من طرف آخر. وكان إنمان يأمل من هذا الحديث، أن يكون مناسبة لشرح وجهة نظر وكالة الأَمن القومي في هذه التوترات، فإذا وعى الناس الحكمة في سلوكه، وافقوا على هذا السلوك.

أنثق بوكالة الأَمن القومي؟ يجيب إنمان بـ «أجل». لقد أصاب جماعته شيء من الحيف مؤخراً، وها هو ذا يتهيأ لوضع النقاط على الحروف. فهل الوكالة هي من ابتدع المواصفات لمعيار التشفير (ديز)، أَو ربما أقحمت فيه باباً سرياً؟ الجواب: ذلك أمر مستحيل. وهل وكالة الأَمن القومي هي من توسل بأَنظمة التصدير لمنع بحث علمي؟ أجل. هل توسَّلت الوكالة، بنفوذها، لإلغاء منح لتمويل البحوث؟ رجاء لا داع للإحراج. ولقد أصر إنمان على أن وكالة الأَمن القومي ليست ـ مهما قيل فيها ـ «بذات القوة الخفية المطلقة لتؤثِّر في كل أمر». بل الحق أن هذه هي عين المشكلة: أي بينما يشكو الغرباء من وكالة جاسوسيَّة ضخمة ذات سلطان عظيم على الكريبتوجرافيا فإن ما يشغل بالي هو: أنَّه ليس للحكومة إِلاَّ أقل مما يلزم».

لقد كان لدى إنمان، على نحو ما، وجهة نظر ممتازة، ومؤداها أن وكالة الأَمن القومي وإن كانت أغنى وكالة استخبارات على هذا الكوكب، ظلّت تقريباً بلا قواطع أَو نواجذ. غير أن الوكالة، لم تكن بحاجة في العقود الأولى من نشوئها لقوانين من وضعها. ولم تكن امتيازاتها لتقتصر على امتلاكها سلطة القانون وحسب بل على كون الكريبتوجرافيا المتطورة حقلاً اختصاصياً لا يلجه إِلاَّ الدهاة، ولم يحاول دخوله إِلاَّ القلة القليلة، وأقل منهم من يستطيع امتلاك المعرفة الكافية ليخوض فيه. ويكاد يكون من العسير تصور الغرباء أَو حتى الحكومات الصغيرة، إمكانية منافسة ما لديها من أجهزة كومبيوتر عملاقة، وعلماء رياضيات أفذاذ على المستوى العالمي، وما تتمتع به من خبرة دونها كل مؤسَّسة أخرى، وفهم لتاريخ الكتابة بالشّيفرة لا يضارعها

فيه أحد. ولكن جاء بعدئذ أمثال هويت ديڤي بالرياضيات ولديهم الكومبيوتر والمعرفة المستقاة من الكتب كالتي وضعها ديڤيد كاهن، ولم تستطع وكالة الأَمن القومي قمعها. والآن، هناك العشرات من هؤلاء، أكاديميون مثل رون رايفست وأشخاص يطمحون لأن يكونوا رجال أعمال مثل كارل نيكولاي. وكان يرفد هؤلاء جهاز من المنادين بالحريات المدنية، وهم يعلنون بأعلى الصوت أن في الكشوفات الكريبتوجرافية ما يكفل توجيه ضربة لطغيان الأخ الكبير [إشارة للدكتاتورية والمجتمع الشمولي في رواية جورج أورويل الشهيرة «1984»]. وفجأة نجد أنّه حتى المحاولات الواهنة، التي قامت بها وكالة الأَمن القومي لوقف التيار جرى تصويرها بصورة شيطانية على الصفحة الأولى من صحيفة النيويورك تايمز. إن الضحية في رأي إنمان، ليست حرية التعبير، وإنما الأمن القومي.

ولكن الحل الذي اقترحه إنمان ـ تضحية على المستوى القومي بحرية التعبير مقابل الحفاظ على الأَمن القومي ـ كان محكوماً عليه بالفشل. كان يطلب الثقة. فإذا أراد أن يقنع الأكاديميين بالتخلي، طواعية، عن حقهم في التعبير، فلا بدّ له من أن ينال منهم الثقة. ولو كانت الثقة عملة، لكان رصيد وكالة الأَمن القومي الصفر تقريباً. والحقيقة، أن الوكالة لم تكلّف نفسها عناء فتح رصيد مصرفي على الإطلاق!

ذلك أن معرفة السبيل للتحكم بوحش الكريبتوجرافيا الذي يزداد شراسة خارج نطاق الحكومة أمر يحتاج إِلىٰ أكثر من خطابات تاريخية يلقيها مدير هو هدف مكشوف لسهام النقاد.

وبقدر ما يتعلّق الأمر بحظر البحث الأكاديمي في الكريبتوجرافيا، فإن إنمان خسر تلك الجولة. وخلاصة ذلك أن القول الفصل ـ بالرغم من كل محاولاته لحمل الكونغرس لمنح وكالة الأَمن القومي السلطة القانونية لحظر طباعة ونشر تلك الأبحاث ـ قد كان للتعديل الأول في الدستور. وكان الأدعى

للتأثير، ما جرى من توضيح استثناء «المطبوعات التقنية» من أَنظمة تصدير الأسلحة إِلىٰ الحد الذي لا يستطيع معه حتى موظفو فورت ميد، التذرع بالالتباس في صياغة النص. وقد جاء في تعديل الأَنظمة الذي تم في عام 1980، أنه «جرى إضافة ما يلزم لإيضاح أن تصدير البرامج التقنية، ينبغي ألا يؤدي إِلىٰ الإخلال بالتعديل الأول لحقوق الأشخاص».

ولقد استطاع بوبي إنمان التوصل إِلىٰ تسوية مع مجتمع الباحثين. وبناء على طلب وكالة الأَمن القومي قام المجلس الأمريكي للتربية، بتنظيم مجموعة دراسة الكريبتوجرافيا لتكون أرضاً مشتركة تجمع الباحثين الأكاديميين وعناصر وكالة الأَمن القومي. وكان أول اجتماع عقدته المجموعة التي ضمَّت المستشار العام في الوكالة ومجموعة من الأكاديميين، بمن فيهم الناقدين مارتي هيلمان وجورج دافيدا في آذار/ مارس 1980، لدراسة اقتراح إنمان، الداعي إِلىٰ إخضاع الباحثين في الكتابة بالشّيفرة من خارج المؤسسات لضرب من الفحص القانوني. وقد رفضت الجماعة الفكرة، استناداً إِلىٰ مضمون التعديل الأول وعجز وكالة الأَمن القومي عن تقديم شاهد على ضرورة مثل هذه القوانين للدفاع عن الأمة. وكان الحل البديل الذي طرحته، هو عملية اختبارية لسنتين تقدم خلالها الأعمال المطبوعة ذات الصلة بالكريبتوجرافيا اختيارياً إِلىٰ وكالة الأَمن القومي للدراسة. فإذا قرأت الوكالة البحث ورأت فيه ما يلحق ضرراً بالأمن القومي فيمكن للباحث عندئذ أن ينظر في المحاذير وله بعدئذ المضيّ في نشر بحثه أَو الإمتناع. ويكون من شأن الوكالة في تلك الفترة، الإستمرار في تمويل البحوث التي يقوم بها المحترفون، الذين يقبلون باتباع لوائحها، تاركة للآخرين الإفادة من التمويل من المؤسَّسة القومية للعلوم، أَو أية هيئة أخرى.

أما جورج دافيدا فقد قدم تقريراً يعبر عن رأي الأقلية، رافضاً حتى فكرة اختيار مراجعة البحوث، ضارباً صفحاً عن أسباب القلق عند وكالة الأمن القومي، بما في ذلك الخشية من استفادة الخصوم من نتائج البحوث في اختراق

أنظمة الكريبتوجرافيا التي نأخذ بها. فكتب معلقاً على هذه الناحية بأن «هذا أمر لا يرجح، لأن الباحثين لا يعملون في تحليل الشّيفرة». وكانت النتيجة التي خلص إليها هي أن «سعي وكالة الأَمن القومي للتحكم بالكتابة بالشّيفرة هو جهد لا ضرورة له، ويؤدي إِلىٰ الانقسام وتبديد الجهود، كما أنَّه أمر يثير الفزع. وتستطيع المؤسَّسة القومية للعلوم النهوض بمهمتها على نهجها القديم بأن: تظل في المقدمة سابقة الآخرين».

ومع ذلك فقد نجحت هذه السياسة من وجهة نظر الباحثين، لأن مؤداها أن ثمة طريقة للتعامل مع وكالة الأَمن القومي ـ أَو تجاهلها ـ دونما قلق من أن تعتبر الحكومة بحوثهم من الأسرار الحكومية التي يجب الحفاظ على سريتها. ولقد مرت فترة اختبار هذه السياسة، بسلام، وتخلّت وكالة الأَمن القومي بعد هاتين السنتين عن أي حق بطلب تقديم أي نتاج يأتي به أكاديمي، للنظر فيه قبل إجازة نشره. وكانت الوكالة تمحص البحوث في هذا الحقل والمقدمة طواعية، ويصادف أحياناً، أن يوجه أحد العلماء فيها سؤالاً للمؤلف، أَو يشير إِلىٰ خطأ تخلّل البحث هنا أَو هناك. وكان ذلك يجري بكل احترام ومجاملة، لأنه لم يكن لوكالة الأَمن القومي أي سلطة لتتجاوز هذا الحد.

ومع بداية الثمانينات، وهو العقد الأول من حياة وكالة الأَمن القومي، حين كان لها منافس في القطاع الخاص، لم يكن هناك من يدرك التحدي المطروح أكثر من بوبي إنمان، الذي كانت الهيئة التي يقوم برئاستها مكلفة باعتراض الاتصالات الأجنبية المتبادلة والمتصلة بأزمة الرهائن في إيران والحرب الروسيَّة في أفغانستان. وكان يؤرق أجفانه أن يجد فورت ميد ذات يوم عاجزة عن توفير مثل هذه المعلومات الثمينة التي كانت تقدِّمها يومذاك، لأن مآل منظومات الكتابة بالشّيفرة التي ابتدعت، وطوِّرت في الولايات المتّحدة أن تصبح شائعة الاستعمال في أغراض التجارة. وقد عبّر عن ذلك القلق بقوله: أخذت أدرك يومئذ خطر التصدير على نحو أشد مما كان يلح علي في

الماضي». وفي عالم يقع المرء فيه على التصورات الأساسية، التي تستند إليها الشيفرة المتطورة في المكتبات العامة ويصادفها في المقالات التي تنشرها مجلة «العلوم» الأمريكية Scientific American، وحيث بدأ يشيع نظام للشيفرة تزكيه الحكومة ذاتها ـ معيار تشفير البيانات (ديز DES) ويحظى بإقبال أشد مما توقعت له وكالة الأَمن القومي، غدا إيقاف شيفرة عند الحدود، أكثر أهمية من أي وقت مضى: إن القضية كلها تتعلّق بالتصدير.

وقد يكون ديفي وهيلمان وثلاثي معهد ماساتشوسيتس، حطّموا احتكار وكالة الأَمن القومي البحث في الكتابة بالشّيفرة، إِلاّ أن إنمان وخلفاءه لم يكونوا يعدمون السلاح للرد. إن حرب الشّيفرة إنما كانت بمعنى ما قد بدأت.

الترويج للشيفرة

أخذت التوترات، في السنوات القليلة التالية، تهدأ بين الحكومة والقوى التي بدأت بالبروز حديثاً في عالم الشيفرة. فبعد حملة بوبي إنمان الفاشلة لغرض الرقابة على الباحثين فيها، بقوة التشريع، بدت الوكالة على استعداد للتعايش، مع أكاديميين أخذوا يخطون على أرض كانت حكراً لها. وربما يكون قد شاب الأمر كله قدر من الأماني الشخصيَّة، وشعور في وكالة الأَمن القومي بأن هؤلاء الأكاديميين الأغرار، من المستبعد أن يأتوا بما قد يهدِّد مهمة «القلعة» بالخطر. ولو اعتقد البيروقراطيون خلف السياج الثلاثي أنَّهم مصدر خطر، لأنكروا ذلك وأبعدوا عنهم هذا الخاطر. ولكن الاكتشافات الأساسيَّة التي تمّت في ستانفورد ومعهد ماساتشوسيتس قد أشعلت منارة هادية عند تقاطع طرق الشّيفرة الوهمي، حيث تلتقي الرياضيات وعلوم الكومبيوتر وسرِّيَّة البيانات. ففي عام 1971، اضطر هويت ديفي للسفر مئات الأميال ليتحدث مع أي شخصٍ مهتمٍّ في أمر الشّيفرة، ثم يحصل على كسرة من المعرفة. وبعد مضي عقد من الزمن، كان هناك أكثر من مئة، من أعضاء جماعة المعنيين بالشّيفرة الجديدة، يمضونَ الأيام معاً على ساحل المحيط الهادي، وهم يتناولون كل أمر بدءاً من الخوارزميات الناجعة إلىٰ تحليل الشّيفرة.

ثم بدأت مؤتمرات «الشّيفرة» في عام 1981 حين دعا أستاذ يدرس الهندسة الكهربائية بجامعة كاليفورنيا بسانتا بربارة، يدعى آلان جيرشو، حوالي 120 شخصاً إلىٰ كليته، وهي مجموعة من المباني المتواضعة تشرف على منحدر يتصل بالمحيط. وكان قد حصل على أسماء مدعويه من قائمة وضعها لين أدليمان، وتشمل أسماء أشخاص أظهروا اهتماماً بالكتابة بالشّيفرة غير الحكومية، وحصل على تمويل هذه المناسبة من منحة قدمتها المؤسَّسة القومية للعلوم. ولقد جاء لحضور المناسبة حوالى مئة شخص، منهم ديڤي، ورايفست، وميركل، وعلماء حديثو العهد في عالم الشّيفرة. وكان أن ألقى هؤلاء أبحاثاً، عرض الكثير منها تحسينات على مخطّطات المفتاح العلني والحقيبة والخوارزمية (رسا)، كما ألقوا كلمات في هذه الموضوعات وكان لهم نصيب من المتعة في تناول الغداء في المقهى، واللحم المشوي في الهواء الطلق. وقد خطّط جيرشو لهذه المناسبة كاجتماع وحيد فريد، وبالرغم من الحماس الذي ساد المناسبة فإن منظمها لم يأخذ في حسبانه الاهتمام بمتابعتها في مناسبات قريبة. ثم لم يمض وقت طويل بعد هذه الندوة حتى كان بعض المعنيين بالكريبتوجرافيا في أوروبا يعقدون اجتماعاً، اقتصر على المدعوين إليه في ألمانيا، إِلاَّ أن هذا الاجتماع أراد له أصحابه أن يكون منتدى للمستقلين.

وكان بين المدعوين في حفلة سانتا بربارة الضخمة، لاعب، ما يزال حديث العهد يومذاك، مجرد خريج دراسات عليا أخذ على عاتقه المبادرة والعمل على أن تجري مثل هذه اللقاءات بصورة دورية. كان هذا الشخص يدعى ديڤيد تشوم، ولكنَّ تواضع حاله في هذا الحقل لم يدم طويلاً. وقد استطاع الحصول دون مساعدة على نسخة من القائمة التي وضعها أدليمان بالأكاديميين المعنيين بالشيفرة، ثم أخذ يعد لتنظيم عودة إلىٰ الجامعة الواقعة على شاطئ المحيط. وقد رأى تشوم كذلك أن من المفيد تكرار ما حدث عبر البحار، إنما بقيادة رواد غير أولئك. ومع أنَّه لم يدع لحضور اللقاء الألماني فقد

تحقق لديه الانطباع بأن الذين قاموا على تنظيمه كانوا «أقرب إِلىٰ اليمين». وهكذا، ما كان منه إِلاً أن اتصل ببعض علماء الشيفرة الأوروبيين يستمزج رأيهم في تنظيم لقاء سنوي في الربيع يكرس «للشيفرة الأوروبية». وأخيراً رأى تشوم أن الندوتين ينبغي أن تعقدا بعناية منظمة حقيقية من الباحثين المستقلين، وأخذ يعد من ثم لتشكيل مثل هذه المجموعة، مهتدياً بخطاب لمارتين لوثر كينج سمعه وهو يشدد فيه على كلمة «التنظيم» كطريق للتحرّر.

ولقد حرص تشوم أن تقتصر اتِّصالاته على الحد الأدنى خشية أن تمارس وكالة الأَمن القومي ضغطاً عليه لخنق مشاريعه في مهدها. فليس ثمة سبيل للمرء ليتحقق من وجود من يصغي إِلىٰ محاوراته، وخاصة في حكومة من الجواسيس. كذلك حرص تشوم على تصنيف المعلومات التي يناقشها مع الناس: ومن ذلك أنَّه وضع رون رايفست في رئاسة مشروع مؤتمر سانتا بربارة، مثلاً، غير أنَّه لم يكشف له عن مشاريعه لإنشاء جمعية لبحوث الشيفرة. ثم إنه كان يتفادى المكالمة بالهاتف مؤثراً اللقاءات مع أولئك الذين يود الاتِّصال بهم. وكان يتولى فضلاً عن ذلك تنضيد نشرات المؤتمر بنفسه ويقوم بطباعتها في المطبعة الصغيرة ذاتها التي تتولَّى طباعة «نشرة المعلومات السرِّيَّة» في بيركلي. وهذه نشرة معروفة بانتقادها نشاطات الولايات المتَّحدة الاستخبارية.

ولقد أتت جهوده أكلها، إذ أن المؤتمر كريبتو 82 فاق الأول إثارة. وكان حافلاً منذ ذلك اليوم بالمناسبات البهيجة مثل «الجلسة البرلمانية» التي عُقدت مع نهاية الأسبوع، ثم غدت تقليداً متبعاً. وكان يقوم على الجلسات البرلمانية عادة هويت ديفي، وتمتزج فيها المعارضات الساخرة بالمحاضرات الرياضيَّة وعرض لأحدث التطورات في كتابة الشيفرة، وغالباً ما كانت بلهجة ساخرة متهكمة. وفي أحد الأعوام، طلب من المحاضرين أن يتكلَّموا بطريقة رمزية، بحيث تستبدل كلمات معينة بأخرى سخيفة تثير الضحك، (كأن تقول «زجاجة كولا» عوضاً عن ديفي ـ هيلمان). وكان المستمعون يقابلون من لم يفهم

الإِشارة برشه بالماء. وفي عام آخر أعلن ديفي عن جلسة خاصة للنكات البلجيكية تمتد تسعين دقيقة قبل الفطور. وفي صباح اليوم التالي أخذ بعض الضيوف الأجانب الإعلان على محمل الجد ونفَّذوه بحرفيته.

وكان من الجلسات المتوقعة في مؤتمر كريبتو 82، عرض لمجموعة من أوراق البحث في تحليل الشّيفرة، تولى رئاستها هويت ديفي؛ لكن وضع هذا الموضوع على جدول الأعمال، لم يكن بالأمر الذي يطيب لوكالة الأَمن القومي: ففي رأي الوكالة أن كل معرفة بتفكيك الشّيفرة خارج السياج الثلاثي يعني تهديداً محتملاً للشيفرات لديها. ولذلك كان ديفي يخشى أن تحبط هذه الجلسات، وفي ذلك تبديد لجهد في الإعداد والتنظيم لهذه المحاضرات أمضى فيه فصل الشتاء بكامله. لكن تلك المحاضرات كان يتم إلغاؤها الواحدة تلو الأخرى ولأسباب مختلفة. ولما حلّ الربيع لم يبق منها سوى محاضرة واحدة بعنوان «قنبلة بليتشلي بارك»، ألقاها أحد روّاد تفكيك الشيفرات في الحرب العالمية الثانية.

ولقد أدَّى مجيء آدي شامير يومئذ لإنقاذ الموقف؛ فشامير كان منكباً على دراسة منظومة رالف ميركل لإنتاج المفتاح العام للشيفرة بواسطة الحقيبة. واعتقد، قبل عدة أسابيع من انعقاد المؤتمر، أنَّه توصل إِلىٰ نسف فكرة ميركل، أَو على الأقل، الصورة الأضعف من النِّظام المعروف بالحقيبة الوحيدة التكرار. وفي الأيام التي أعقبت هذا الإعلان ابتكر آخرون طريقة لتطبيق أساليبه ـ التي تعتمد على ابتكارات في الرياضيَّات اكتشفها هندريك لينسترا ـ لشن هجمات أوسع نطاقاً. وكانت ندوة ديفي المناسبة المثالية لاختبار هذه الأفكار. وهكذا ما إن التأم اجتماع الكريبتوجرافيين في سانتا بربارة في ذلك الصيف، حتَّى كان برنامج ديفي حافلاً بالمحاضرات التي تتناول الحقائب بالنقد.

وكان أكثر تلك الانتقادات مدعاة للاهتمام ما جاء به لين أدليمان. فهو لم يقتصر على تقديم معالجة مختلفة للأفكار التي ينادي بها شامير بل زاد بأن قام

ببرمجة طريقته على الكومبيوتر الخاص به وهو من طراز أبل 2 الشخصي. وشاء الكريبتوجرافيين في سانتا بربارة إجراء تجربة صغيرة. ففي أول أمسيات المؤتمر، رمى هؤلاء بقفاز التحدي في وجه أدليمان، وكانت رسالة مشفَّرة بطريقة الحقيبة: فهل يتمكن من فك شيفرة الرسالة بجهازه الصغير؟ (ولو استطاع لكسب جائزة المئة دولار التي سبق أن عرضها ميركل قبل بضع سنوات). وكان أمامه يومان للإجابة عن هذا السؤال، في مكان الجلسات التي يرأسها ديڤي، فإما أن يخرج مكلّلاً بغار النصر، أَو يسقط هناك مهزوماً أمام أقرانه.

كان مقرّراً في جدول الأعمال أن يكون أدليمان آخر المتكلمين. ويتذكّر ديڤي المناسبة ويصف وقائعها قائلاً: «مضت الساعة، وسمع الحاضرون مختلف الأساليب التي تتناول منظومات الحقيبة على اختلاف مواصفاتها؛ وكان كومبيوتر أدليمان جاثماً على الطاولة، والجميع ينتظرون أن يطلع عليهم بما أتت به جهوده». ولما تقدم أدليمان للحديث بدا للحضور متردداً. وقال يومئذ أنه «سيعرض النظرية التي يستند إليها أولاً، ثم يتلقى مهانة الفشل بعد ذلك». (وقد قال لاحقاً أن المهانة التي قصدها لا تصل بميركل وإنما بما سيناله هو، إن «أخطأت الأَرقام»). ثم تابع كلمته بعرض المناهج التي يعتمدها. وفيما كان يمضي في حديثه كان كارل نيكولاي (مخترِع جهاز للتشفير وقع عليه حظر مؤقت بموجب أمر سري أصدرته وكالة الأَمن القومي عام 1978)، يعبث بالكومبيوتر الذي كان يعمل طوال الأيام الماضية، لتفكيك الرسالة المشفَّرة، باستخدام صيغة أدليمان. وكان نيكولاي يقوم بنسخ أَرقام امتلأت بها شاشة الكومبيوتر على شفافيات جهاز إسقاط.

وأخيراً أنهى أدليمان حديثه بعرض طريقة تنفيذ هجومه لتفكيك الشّيفرة. وهنا آن أوان اختبار الطريقة. قدم نيكولاي الشفافيات إلىٰ أدليمان الذي سلمها بدوره إلىٰ شامير، كما قدم له المغلف المختوم مع الرسالة التي سبق تشفيرها في المؤتمر. وهنا وضع شامير الصفحتين بجانب بعضهما في جهاز الإسقاط

لإظهار النتائج على الشاشة. ولقد جاءت الصورتان، النص المشفَّر والنص الواضح، متطابقتين تماماً.

وكتب ديفي فيما بعد: «إن المهانة المشهودة لم تنزل بأدليمان، وإنما كانت من نصيب الحقيبة». حقاً إن هذا التفكيك كان الضربة الأخيرة التي ستأتي لاحقاً على ذلك الفتح الخارق، وغير المجدي والمتمثِّل في المفتاح العام لنظام التشفير المعتمد على الحقيبة. والحق أن ميركل ذاته هو من دعا إلى إطلاق رصاصة الرحمة على مشروعه. وإن دفعْ مئة دولار لأدليمان لم يكن بالأمر الفاجع؛ فلقد خامر ميركل شيء من الشكّ بأن يتمكّن أحدهم من اختراق الحقيبة وحيدة التكرار، وهي ابنة عم للحقيبة الأصلية المتعددة التكرار، ودونها إحكامَ بما لا يقاس. والواقع أن ميركل كان واثقاً من نتاجه إِلىٰ الحد الذي جعله يطرح تحدياً آخر. ففي تشرين الثاني/ نوفمبر من ذلك العام وجّه رسالة إِلىٰ مجلة «تايم»، يعرض فيها تقديم ألف دولار لأول محلِّل شيفرة همام، يفلح في تفكيك الحقيبة متعدِّدة التكرارات. وكان أن اضطر ميركل لتوقيع شيك بهذا المبلغ جزاء لباحث يدعى إيرني بريكيل وهو الذي استخدم كومبيوتراً عملاقاً من أجهزة الحكومة لفتح حقيبة أربعينية التكرار. ولما سئل ميركل عن المشكلة في مخطط الحقيبة المتعددة التكرار، كان الجواب مختصراً: «لم يعمل».

ولقد كان لهذه الهجمات على الحقيبة مغزى أبعد من تداعي منظومة ميركل. فالواقع أنه يمكن النظر إِلىٰ اللحظة التي نسف فيها الكومبيوتر الشخصي على يد لين أدليمان، نظام شيفرة ثمين في حدّ ذاته على أنَّها نقطة تحول رمزي في الميزان الذي ما زال على اضطرابه بين جبابرة الشيفرة المرتبطين بوكالة الأَمن القومي والأعداد المتزايدة من الغرباء الذين درسوا أصول الشّيفرة، وجروا على نشر نتائج دراساتهم. وكان واضحاً الآن، أنه يكفي مجيء العلماء إِلىٰ مؤتمر والاشتراك في دوريات قليلة. حتَّى تتمكَّن أية حكومة أجنبية من الحصول على ذلك النوع من التدريب على الشّيفرة، الذي كان مقصوراً من قبل

على النخبة المجاز لها. وكان معنى ذلك أن مفككي الشّيفرة يستطيعون في أي مكان زيادة نصيبهم من المعرفة والخبرة. فقبل أشهر قلائل فقط، وجدنا منتقد الحكومة جورج دافيدا يسخر من الدعوات التي أطلقتها الوكالة لإخضاع الأبحاث المقدمة للنشر لدراستها قبل إجازتها بتشديده على أن أعظم أسباب القلق لدى الحكومة، هي أن يأخذ من هم غرباء عن المؤسَّسة الرسمية في نشر طرق تفكيك رموز الشّيفرة، هو أمر من قبيل السخف. وقد عبَّر عن ذلك بقوله أن «الباحثين لا يشتغلون بتحليل الشيفرات».

إن البعض في وكالة الأَمن القومي قد أدرك الخطر الذي يحمله وجود جماعة مستقلّة من المشتغلين بالشّيفرة، وتجلى ذلك باتِّصال أحد هؤلاء بديفي ليقول له بلهجة كئيبة إن المشكلة ليست في أننا لم نر هذه المنطقة من قبل، وإنما في أنكم تأخذون في مسحها بسرعة شديدة».

وكان الأمر الوحيد الأسوأ من هذا عند وكالة الأَمن القومي هو رؤية هؤلاء الأكاديمين يعملون في تطبيق هذه المعرفة عملياً، فإذا أمكن إقامة صناعة على أساس الإفادة تجارياً من الشّيفرة، وشرعت جماهير الناس في استخدام تقنيات الترميز، فلسوف تتحوّل عندئذ الإشارات الواضحة غير المشفَّرة التي تعترضها أجهزة الإصغاء في وكالة الأَمن القومي، سواء كانت مكالمات بالهاتف الخليوي أم رسائل ترسل بالبريد الإِلكتروني أم ملفات كومبيوتر - إلىٰ ضجيج مزعج، وأصوات متنافرة قد تفلح الكومبيوترات في الوكالة، في تبديد ألغازها بشيء من الجهد. أَو لعلها لا تفلح في ذلك.

وكان السؤال التالي: هل ثمة إمكانية لتحويل الشّيفرة إلىٰ سلعة تجارية؟ فلئن كان استخدام الكومبيوتر الشخصي، ثم الإنترنيت، لاحقاً، بحاجة إلىٰ طريقة لحماية المعلومات والتثبت من مرسلها، فإن الطريق لبلوغها كان في أفضل الأحوال غير معبَّد. وأفضل ما يصور حال تلك الحفر والأخاديد التي تعتور هذا الطريق ما كان من مصير الشركة التي أنشأها رون رايفست، وآدي

شامير، ولين أدليمان. وكانت هذه الشركة تحمل الحروف الأولى من أسماء أصحابها، كما كان شأن الخوارزمية الرائدة التي طلعوا بها. ولكن بينما أصابت الخوارزمية «رسا» نجاحاً سريعاً وبلغت الجمهور الذي تحمّس لها، وجدنا مبدأ مسار العمليّة التجارية يذكّر بعمليّة إطلاق صاروخ فاشلة.

والواقع أنّه لم يكن في مطلع الثمانينات ما يشجّع كثيراً على الاعتقاد بأن هذه التكنولوجيا ستأتي بربح كبير، بالرغم من التوقعات المتفائلة التي حملتها أبحاث ديفي ـ هيلمان ورايفست ـ شامير ـ أدليمان بنهضة في كتابة الشيفرة. فمن تراه يغامر بالرأسمال لتمويل إنتاج المكونات اللازمة لها؟ وكيف يمكن تركيب هذه المكونات لتشكل منظومات، بحيث يطمئن المرء بأن الرسالة المشفَّرة يمكن تفكيكها فعلاً، أَو أن متلقي التوقيع الرقمي سوف يكون لديه العدة اللازمة للتثبت من صحته؟ الحقيقة، أنّه لم يكن هناك من يدري إن كان الزبائن الفعليون على استعداد لاحتمال المصاعب التي تنجم عن معالجة الكومبيوتر، لأَرقام ضخمة في عمليات التشفير والتثبت من صحة الرسائل والتوقيع أم لا. والواقع أنه لم يكن هناك من يعلم إن كان ثمة ما يكفي من الزبائن المستعدين لدفع التكاليف المترتبة على هذه العمليات. وقد عبّر رايفست عن هذا الوضع بقوله: «هناك من قال أن منتجنا ربما كان ذا فائدة، ولكن لم يكن واضحاً إن كان المشروع سيصيب نجاحاً بالمعنى التجاري للكلمة».

ومع ذلك، فقد عمدت الجامعات التي وظفت لديها باحثين في الكريبتوجرافيا، إِلىٰ تدعيم مراهناتها على نتاج هؤلاء بطلب للكلية للاكتشافات التي حقّقوها في اختراع المفتاح العام. ففي كانون الأول/ ديسمبر 1977، تقدم معهد ماساتشوسيتس بطلب براءة الاختراع عن الخوارزمية «رسا». وكان من قبيل المفارقة المضحكة المبكية أن الطلب عينه جعل الإقبال على تبني مشروع الكريبتوجرافيا أمراً مستبعداً. فقد كان الادعاء بالملكية الفكرية ينطوي على حرج منطقي: فإذا كان يمكن إجازة الخوارزميات كملكية فردية، فإنّه لا يمكن

استخدامها إِلاَّ من قبل أولئك الذين حصلوا على إجازة بذلك من أصحابها (لقاء أجر كما يفترض). غير أن مثل هذه التصرفات كفيلة بأن تحمل على العزوف عن تبنيها على نطاق عالمي. وإذا كان يُراد الإفادة من الكريبتوجرافيا على نطاق واسع، فمن المنطقي والحالة هذه، أن يقبل الجميع على استخدام منظومة واحدة بعينها، وهو التقاء كان يتحقق بسرعة أعظم لو كان النِّظام يُقدم مجاناً. وكان هذا مثالاً كلاسيكياً على «تأثير الشبكة»، وهو حلقة تغذية استرجاعية لا تكون له فائدة إِلاَّ إذا شاع وتعمم. ذلك أنه سيكون من العسير قيام التواصل سراً مع الآخرين، إن لم يأخذ الجميع بخوارزميات واحدة؛ ومثل هذا مثل امرئ أراد مكالمة شخص، فإذا به لا يدري أي هاتف يستعمل صاحبه هذا.

وليس مؤدى القول أن المؤسَّسات التي قامت بتمويل الأبحاث في المفتاح العام قد أزعجها هذا الحال. ففي حين لم يكن معهد ماساتشوسيتس ليملك سوى الملكية الفكرية لـ «رسا»، كانت جامعة ستانفورد تتمتع بعدة براءات ملكية، وهي تتراوح بين الادعاء العام بملكية مفتاح عام حتَّى التطبيقات المحددة، بما في ذلك أصول مفتاح ديڤي ـ هيلمان ومخطط حقيبة ميركل.

ولكن الفوائد المتحقّقة من امتلاك براءة الاختراع كانت محدودة: ومن أسباب ذلك أن السوق الأوسع حالياً ـ أعني الحكومة ـ لم تكن تجد ما يحملها على دفع ثمن لاستغلال أي من الأَنظمة التي أنتجت في جامعة ستانفورد أَو معهد ماساتشوسيتس للتكنولوجيا. ذلك أنَّه لما كانت كلتا الجماعتين العاملتين في الكتابة بالشّيفرة قد تمتعت بدعم المؤسَّسة القومية للعلوم فإن القانون يسمح لأي هيئة أَو مجموع هيئات الحكومة الاتحادية، بأن تفيد دوماً من ثمار الأبحاث المموّلة. ولزيادة الطين بلة ظهر أن براءات الاختراع الخاصة بجامعة ستانفورد، والخوارزمية رسا، لا تسري إِلاَّ على الولايات المتّحدة وحدها. وفي حالة الاختراعين، كان الباحثون قد عرضوا نتائج بحوثهم قبل طلب براءة الاختراع، فكان أن أدى ذلك الخطأ الناجم عن جهل، وإن لم يكن له أثر على

حقوقهم الأدبية في الولايات المتّحدة، إِلىٰ حرمانهم من الحماية في أوروبا (مما سببه نهج التعامل مع براءات الاختراع في الخارج).

ومع ذلك ما إن بدأت طلبات براءات الاختراع تجري على قدم وساق، حتّى اتضح لرايفست وشامير وأدليمان أنهم ما زالوا يتمتعون بحرية استثمار هذه الإجازات. وكان معهد ماساتشوسيتس معروفاً بالسخاء في منح ملكياته الفكرية للأشخاص الذين لهم الفضل في ابتكارها فعلاً. (ولو كان شأنها غير ذلك لجازفت بإثارة ثورة الجامعيين عليها). غير أن هذا الثلاثي واجه وضعاً فريداً: فلقد كان لمشروعهم لكتابة الشّيفرة الإمكانية لأن يصبح معياراً عالمياً لتأمين السرِّيّة، والرواج تجارياً، لولا أن التجارة الرائجة الوحيدة كانت، حتّى ذلك الحين، محصورة في هذا الحقل بمجال المقاولات التي تتصل بمشاريع الدفاع والسوق الجديدة نسبياً للمنتجات مثل معيار تشفير البيانات الذي راج عند المؤسَّسات المالية. وعلى كل حال لم يكن أي من هؤلاء الباحثين الثلاثة يتمتع بأية خبرة تجارية. ولكنَّهم عزموا على المضي قدماً في هذا الاتجاه، آملين أن يصنعوا من فتوحاتهم الرياضية ما يمكن للبشر العاديين استخدامه للتفاهم فيما بينهم. كانت آمالهم عظيمة بالنجاح في هذا السبيل، وكان منهم واحد على الأقل يعتقد بأنَّهم قاب قوسين أو أدنى من جني الثمار. وكان هذا لين أدليمان، الذي أسرع إِلىٰ شراء سيارة تويوتا حمراء زاهية، وراح يتباهى بها: «لقد كلفتني ثلاثة أَو أربعة آلاف دولار. وهذا مبلغ ضخم، فدخلي كان حوالي الثلاثة عشر ألف دولار في السنة. غير أنني اعتقدت يومذاك أني سوف أحصل على مال وفير في المستقبل القريب فأتخلى عندئذٍ عن هذه السيارة [واشتري سيارة أخرى أفخم منها]».

كان من بين المشكلات التي ظهرت في عقد السبعينات [من القرن العشرين] أن أجهزة الكومبيوتر الشائعة كانت أضعف من أن تولد خوارزميات تشفير جيدة مثل رسا. ولكي يتمكن الأساتذة في معهد ماساتشوسيتس

للتكنولوجيا من إجراء الحسابات اللازمة لتوليد الأَرقام الأولية الضرورية لإنتاج المفتاح، وكافة العمليات الرياضية المطلوبة لتشفير وتفكيك الشّيفرة والتحقق بالكفاءة اللازمة، كان عليهم بناء كومبيوتر صغير داخل الكومبيوتر. فشرع رايفست بمساعدة زملائه، بالعمل لإنتاج مثل هذا الجهاز. فخرجوا بعد شهور من العمل بعتاد يستطيع سحق زوج من 50 رقماً أولياً في أقل من ثانية.

ثم جاءت لحظة مواجهة الحقيقة. وتبين يومئذ استحالة أن تصبح لوحات الدارة المرتفعة التكاليف نسبياً، منتجاً يمكن تسويقه بالجملة. وكان من السخف الاعتقاد بأن هناك الملايين من الناس المستعدين لدفع مئات الدولارات من أجل تركيب لوحة دارة معقَّدة داخل أجهزة الكومبيوتر لديهم، للمشاركة في ثورة يصعب عليهم الإحاطة بأسبابها والنتائج التي سوف تتمخّض عنها.

ولذلك خرج الثلاثي، في عام 1981، بسيناريو أقرب إِلىٰ الواقع. بأن يضعوا الخوارزمية رسا على رقاقة، فالرقاقات المصنوعة من أشباه الموصلات يمكن إنتاجها بكثافة، وإذا أمكن إنتاج الملايين منها، فإن كلفة الإنتاج سوف تتقلَّص. بل إن بوسعك حتَّى أن تصنع رقاقات دقيقة على بطاقات ذكية بحجم بطاقات الاعتماد المصرفية، ويستطيع الناس حملها معهم أينما ذهبوا.

ولقد بدا التوقيت لهذا العمل مناسباً، فقبل بضعة أعوام، حينما استخدمت شركة آي بي إم قدراتها الضخمة لتحقق إنجازاً تاريخياً بوضع خوارزمية معيار تشفير البيانات على رقاقة، لم يكن ليخطر بالبال أنه يمكن لقلة من الأكاديميين القيام بمثل هذا العمل الخارق دون مساهمة عدد كبير من المستثمرين. فقد كان احتمال تحقيق هكذا إنجاز في تلك الأيام، بعيداً بعد احتمال قيام قلة من خريجي الدراسات العليا في كلية من كليات الهندسة بإطلاق صاروخ إِلىٰ القمر. ولكن كان هناك أستاذ في جامعة بكاليفورنيا يدعى كارفرميد، خرج في تلك الفترة وقلب الوضع كله. وكان ميد هذا، من العاملين

القدامى في صناعة أشباه الموصلات في مركز الصناعات الإِلكترونية سيليكون فالي وشيخ الدمج الواسع النطاق VLSI وهي تقنية أدَّت إِلىٰ تقليص ما كان ذات يوم كومبيوتراً ضخماً، ليصبح رقاقة بحجم الظفر. ولقد قام ميد بنشر كتاب في هذا الموضوع، وعمل على إقامة منشأة صناعية ـ تعرف بالفابريكة (فاب) ـ لمساعدة الأكاديميين على صنع رقاقاتهم، سعياً منه للتشجيع على البحث في هذا المجال. وكان معهد ماساتشوسيتس ينهض ببرنامج البحث في الدمج واسع النطاق VLSI، وانضم إليه رايفست ليقوم على مشروع تجريبي يهدف إِلىٰ طبع الخوارزمية «رسا» كلها على إحدى هذه الرقاقات.

وفي تلك الأثناء ثابر الباحثون على ما أصبح جهداً متواصلاً، إن لم يكن كوميدياً عن غير قصد، لاجتذاب اهتمام أحد أباطرة التجارة والأعمال ـ أي واحد منهم ـ بإمكانات الاستثمار في عالم كتابة الشّيفرة. وكعباقرة في الرياضيات لا دراية لهم بطقوس الاستثمارات وبلا تأهيل في حمل الوجوه الخالية من كل تعبير كما يلزم في المفاوضات، والمساومات كان هؤلاء تحت رحمة أي رجل أعمال ترمي به الصدف أمامهم. غير أنَّهم كانوا يصادفون أحياناً شخصاً له معرفة بالمصلحة، وكان من هؤلاء: بات كريمين، وهو إيرلندي ذرب اللسان، يعمل في شركة إيريكسون للإِلكترونيات الضخمة. ولكن بات كريمين هذا كان أيضاً من أصحاب الرؤى، أكثر منه باحثاً عن الصفقات المربحة. وهكذا ما أن اطلع على الخوارزميات التي طلع بها طاقم معهد ماساتشوسيتس، حتَّى انطلق يشدو معلناً حلول عهد من حافظات النقود الإِلكترونية وما هو في حكم النقود. ولقد سحر رايفست وزميلاه بتلك الرؤى، ولعلهم أخذوا يعدون، ويحصون الثروات الطائلة التي سوف تدخل محافظهم الرقمية يوم يطل هذا العالم الجديد. وما كان منهم إلاَّ أن أعدوا العدة ورحلوا إِلىٰ دبلن لمتابعة الفكرة. ولئن أفاد الجمعية، الإعجاب المتبادل في تدعيم معنويات هذه الجماعة، فإن الأحداث أظهرت أن الأمر لا يعدو كونه كذلك،

مجرد دعم معنوي. فقد عجز كريمين بعد محاولات كثيرة عن إقناع رؤسائه في إيريكسون بالاستثمار في هذا المشروع.

ولعل أولئك الرؤساء كانوا على صواب في قرارهم: بعدم توظيف أموال الشركة في هذا المشروع. وهناك طرفة جديرة بالرواية منذ ذلك العهد: ففيما كان جهابذة معهد ماساتشوسيتس يعملون على تنفيذ خوارزمية «رسا» على الرقاقة، إذا بهم يجدون أنفسهم على حافة تصميم رقاقة دمج واسع النطاق VLSI. وكان عليهم أن يبتكروا أدواتهم الخاصّة التي غدت ملكية فكرية ذات شأن في حدّ ذاتها، وهي أدوات تنشد الشركات الضخمة حيازتها، ويسعى الجواسيس الأجانب وراءها. فمثلاً كان على رايفست لمتابعة مئات آلاف البوابات المنطقية والترانسيستورات في تصميم الرقاقة، أن يضع برنامجاً معقداً لمحاكاة الرقاقة ليستقيم المشروع. ولقد جعل برنامجه، الأمور أيسر عند التعامل مع الفوضى التي كان العلماء يثيرونها في الطابق الخامس في مبنى تيك سكوير، عند نشر المخططات الهائلة للرقاقة والقطع التي قام أدليمان بتصميمها، وتولى رايفست رسم هياكلها، فضلاً عن القطع الأخرى التي ابتكرها شامير لمتابعة مسار هذا السلك أو عمل ذاك الترانسيستور؛ وكان ذلك قد يسر هذا الأمر بين التعقيدات ما جعل الثلاثي يعتقد أن البرمجة التي كانوا يستخدمونها في ابتداع الرقاقة قد تنطوي على فائدة تجارية أو عسكرية كالخوارزمية (رسا) ذاتها.

ولقد وجد هؤلاء أنفسهم بإنتاج هذه الملكية الثمينة، في وضع أخذوا يتخيلون فيه حالهم كحال زبائنهم ذات يوم، يملكون أسراراً ثمينة جديرة بأن تُحمىٰ وتُصان، وأخذوا يفكِّرون في ابتكار منظومة خاصة لحماية هذه الأسرار. وهكذا كان أن جلس هؤلاء الثلاثة مع بعضهم ذات ليلة وأخذوا يتداولون فيما بينهم في أمر حماية أفكارهم الثمينة من التسرّب... وكان الأسلوب الذي خطر ببالهم هو التشفير. فهل استخدم هؤلاء الرواد في كتابة الشّيفرة منظومتهم فعلاً

لحماية أفكارهم؟ يقول أدليمان: «أذكر أننا لم نأخذ بهذه الفكرة، ففيها كثير من العناء... وتفرض علينا بذل جهد كبير في التشفير. وهذا عبء لم نكلف أنفسنا به» ولقد فاتهم أن يلاحظوا المفارقة في هذا القرار. غير أن الواقع هو أنّهم ظلوا يعقدون الآمال منذ عهد بعيد على قيام تكنولوجيا يرى حتّى مبتكروها، أنها تكلفهم ما لا يطيقون!.

لقد نظر جميعهم إلىٰ نظام رايفست في محاكاة الرقاقة على أنّه آية من آيات الإبداع. ويقول أدليمان في تصوير تلك الحالة: «إننا لم نرم بهذا [الابتكار] ونحن نأمل بأن يأتي بحل مئات الآلاف من الأمور، فبرنامج رون [إنما] قام بمحاكاة الرقاقة حسب القواعد التي وضعها ميد». ولأن المحاكاة كانت سليمة، يقول أدليمان «كنا واثقين من أن الرقاقة سوف تؤدي عملها المطلوب».

ولكن الرقاقة الحقيقية لم تنجح عند الامتحان. فبدلاً من سحق الأَرقام الأولية، وقفت الرقاقة بدلا من ذلك، في حالة من الإحباط. وفي هذا يلقي أدليمان اللوم لهذا الفشل على المبالغة في الاعتماد على كتابات كارفر ميد، «فالقواعد التي تضمنها كتابه، كما يقول أدليمان، لم تكن كاملة». ولكن إنصافاً لميد ـ وهو لم يكن يعمل في خدمة ثلاثي معهد ماساتشوسيتس، على كل حال ـ كان مشروع الخوارزمية «رسا» أشد ضخامة من أي أمر خطر بباله. ففي حين كان ثمة باحثون كثر آخرون يعملون بإنتاج مشاريع صغيرة مثل رقاقات لإنارة مصابيح الشوارع، كان جماعة معهد ماساتشوسيتس يستخدمون خوارزميات رياضية متقدّمة تتعامل مع أَرقام أولية هائلة وعمليات حسابيّة لا عدّ لها ولا حصر، لاختيار المفاتيح وتشفير نص أَو تفكيك نصوص مشفَّرة وابتكار مفاتيح عامة، والتأشير على رسائل بتواقيع رقمية. والحقيقة، أن الكثير كان يجري على «أسلاك» السيليكون في الرقاقة، حتّى لتعتبر بمعايير التكنولوجيا الدقيقة بالغة الطول، أَو ما يعادل الكابل البحري بين أوروبا والولايات

المتّحدة. وهذا ما يسَّر رصف خيوط السيليكون الدقيقة قريباً من بعضها، مثيرة بذلك «أحاديث متقاطعة» قاتلة من شأنها إفساد تراتب البتات وإجراء الحسابات. وذلك أمر لا ترغب فيه حين تجري مسائل رياضيَّة دقيقة.

يقول رايفست وهو يتنهد من أعماقه: «كانت محاكاة الرقاقة مثالية، ولكن عند التنفيذ لم تأت لنا برقاقات ناجحة. ولعل الأمر كان بحاجة إِلىٰ قرص تصميم المعالج قليلاً». وبعبارة أخرى، لئن كانت التجربة فاشلة من الناحية الفنية، فإن رايفست كان واثقاً من نجاح المخطط في إنتاج نموذج عملي، بالأمر الذي يسمح للمرء بأن يعتبره حافزاً يشجع الآخرين على الشراء.

ومع ذلك فقد ظل العلماء الثلاثة على دأبهم وإصدارهم. ففي عام 1983 انضم هذا الثلاثي رسمياً إِلىٰ عالم التجارة عبر شركة دعوها آر إس إيه داتا سيكيوريتي إنكوربوريتيد RSA Data Security, Incorporated، (وكان أصحاب الشركة يودون أن يطلقوا عليها اسم آر إس إيه وحسب، لو أن هذا كان اسم شركة تختص بجمع القمامة في ولاية ماين. لكن الشركة كانت تفتقر للمُنتج والزبائن، بل لم يكن لديها ما ينبئ بوجود طلب على إنتاجها. والحقيقة، أنّه لم يكن ليراود الشركاء الثلاثة حلم باحتمال استخدام ملايين الناس يومياً للتكنولوجيا التي تقوم شركتهم الجديدة بإنتاجها.

وهنا كان لين أدليمان قد سئم العملية كلها. لأنّه كان يشعر بازدياد بعده عن المجال الذي تبرز فيه مواهبه، أي الرياضيَّات النظريَّة. فقد كان يعتقد أنه من الأجدى له توجيه هذا الجهد الفكري الذي يبذله في حشر الصيغ في رقاقات السيليكون، إِلىٰ محاولة اكتشاف آخر نظريات فيرما أو ما شابه من التحديات الضخمة. ومع ذلك، فقد ظل على التزامه، آملاً أن يفيد هو وزملاؤه من جهودهم، إن استطاعوا أن يشيدوا شركتهم الجديدة على أساس تجاري راسخ. ثم يكون لأدليمان، على الأقل، أن يلتفت إِلىٰ شغله الشاغل، ليملأ،

ـ والسرور يغمره ـ الألواح البيضاء بمعادلات دقيقة لا تنطوي على أي فائدة تطبيقية.

ولقد كانوا يعلمون كرياضيين أن مبدأ أوكام يسري هنا، وهو أن الحل الأقصر للمشكلة هو بسلوك طريق مستقيم إليها. أما في عالم الواقع المبهم هذا الذي يهدف إلىٰ إنجاح مشروع تجاري، فهناك التفافات واستدارات لا تُعدّ ولا تحصى، للوصول من نقطة إلىٰ أخرى. ويصف أدليمان مبلغ حيرة جماعته أمام هذا الوضع بقوله، أنهم كانوا يسيرون «دونما إشارة أَو هدي في هذا العالم». كان أول مدير عام للشركة هو أدليمان ذاته، وقد قبل القيام بهذه المهمة وهو عازف عنها، مع أن عقله يبلغ صفاءه حينما يحلق في السحاب. ويخبرنا اليوم بحاله يومذاك: «كنت المحرك الرئيس في أحوال مختلفة، ورون في أحوال أخرى». (كان شامير يعد نفسه للعودة إلىٰ إسرائيل للعمل في معهد وايزمن، فلم يكن بالتالي بذات القدر الذي كان عليه زميلاه من النشاط). ولقد تصور أدليمان عن سذاجة أنه يستطيع قيادة هذه السفينة الإضافية في لحظات فراغه التي يتيحها عمله الجديد كأستاذ مشارك في قسم الرياضيات بجامعة جنوب كاليفورنيا.

غير أن الجماعة أدركوا حاجتهم لشخص ذي خبرة وتجربة ليسدي لهم المشورة. وقد صادف أن التقوا يومذاك بمشاور في مجال التجارة يدعى تيد آيزن الذي استطاع أن يأتي بما عجز عنه الأساتذة الجامعيون اللامعون مجتمعين. ولقد أمل هؤلاء الثلاثة من آيزن أن يأتي لهم بالمستثمرين سريعاً. وكانت التوقعات تتجه إلىٰ أن الحكومة سوف تمنح معهد ماساتشوسيتس، بعد شهور من التأخير والدراسة، براءة الملكية الفكرية عن الخوارزمية «رسا». وكانت البراءات الخاصة بجامعة ستانفورد قد صدرت قبل ذلك: البراءة الفكرية عن «أداة ومنهج في الشيفرة»، مؤرخة في 29 نيسان/ أبريل 1980، باسم ديفي وهيلمان وميركل، باعتبارهم مخترعي المفتاح العام. ثم صدرت براءة أخرى بتاريخ 19 آب/ أغسطس، خاصة بالأبحاث التي جرت في جامعة ستانفورد،

عن بحث هيلمان وميركل بعنوان «أداة ومنهج المفتاح العام في الشّيفرة»، وقد عالج تحديداً موضوع الحقيبة المنتفخة، ولكنّه تضمن الإدعاء عموماً معالجة تطبيق فكرة المفتاح العلني.

كانت البراءة المتوقعة لمعهد ماساتشوسيتس تقوم على براءات الملكية الفكرية التي حصلت عليها جامعة ستانفورد وتشمل الخوارزمية «رسا». وإذا كان مقدراً للشركة الجديدة أن تحقّق نجاحاً، فلا بدّ لها من أن تحوز على حقوق ملكية ذلك الابتكار وتحصر بها؛ وبدون ذلك يستطيع المنافسون الأطول باعاً وأرسخ قدماً، الحصول على الترخيص اللازم للخوارزمية «رسا» من معهد ماساتشوسيتس، فيطيحون بالشركة التي قام بتأسيسها فعلاً من منحها اسمها من الحروف الأولى من أسمائهم. وهنا كان للمعهد فضله العظيم. فقد وافقت الجامعة على منح رايفست وأدليمان وشامير حق الملكية الحصرية لابتكارهم مقابل 150 ألف دولار. (تلكم هي حدود الفضل والكرم). ولكن من أين لمدرسي الرياضيات الشباب هؤلاء أن يأتوا بمثل هذا المبلغ؟

وجاء آيزن بالجواب: من طبيب ورجل أعمال في رينو، بولاية نيفادا، يدعى جاك كيللي. وكان كيللي هذا يملك شركة تسمى «سييرا مايكروسيستمز» في منطقة بحيرة تاهو، وتختص بتصميم الرقاقات، ورأى آيزن أن ثمة إمكانية بأن يصبح كيللي شريكاً في هذه الشركة الجديدة. وفي ذات يوم طار كيللي بطائرته الخاصة إلىٰ بير بانك للقاء الثلاثي «رسا». ولقد كان الجانب اليسير من الأمر للعلماء الثلاثة إقناع الرجل بالأهمية القصوى لتقنية مثل الخوارزمية «رسا» في عصر المعلومات الذي بدأ بالبروز. أما الجانب الأصعب فكان في عقد صفقة يطمئن إليها رجال الأعمال المستجدون هؤلاء، فلا يصيبهم الندم في الصباح علىٰ ما فعلوا في المساء. ولقد نظر أدليمان إلىٰ الأمر فيما بعد نظرة تأمّل فلسفيّة، بعيداً عن طغيان المشاعر في تلك اللحظة: «كان [كيللي] رجل أعمال مجرباً، وكنت أنا رجلاً حديث العهد بالتجارة والأعمال. فإذا اجتمع هذان الاثنان كانت النتيجة في أغلب الأحيان، اكتساب الغر بعض الخبرة».

ومع ذلك فقد وفّر كيللي المبلغ المطلوب المؤلف ـ من ستة أرقام ـ 225000 دولار، واللازم لبقاء شركة آر إس إيه داتا سيكيورتي. وهكذا كان المستثمرون على أهبة الاستعداد لدفع هذا المبلغ، حينما منحت الحكومة الأمريكية معهد ماساتشوسيتس براءة الملكية الفكرية ذات الرقم 4,405,829، في أيلول/ سبتمبر 1983، عن الاختراع: «نظام ومنهج الاتّصالات بالشيفرة». وما أن انقضت تسعة أيام على هذا الحدث حتّى قامت الشركة الناشئة بدفع مبلغ 150 ألف دولار (بالإضافة إلى 5 بالمئة عن كل مداخيلها في المستقبل)، لقاء حقوق الملكية الفكرية عن الاختراع.

وهكذا كان الوقت قد حان لتقوم الشركة، وقد توفر لها المادة للاستثمار والسيطرة على ملكيتها الفكرية فعلاً، لتتصرّف كشركة تجارية تقوم بصنع أدوات الشّيفرة المأمونة غير القابلة للتفكيك، لمن يملك كومبيوتراً ويرغب باقتنائها. فكان أن أنشأت الشركة بما تبقى من الرأسمال الذي أودعه كيللي مكتباً لها في وادي سيليكون، ثم قامت بتوظيف مدير خبير لإدارة الشركة. وكان لهذا الرجل سجل ذاتي ملفت للأنظار، إذ سبق له أن عمل في شركات ذات مكانة تحظى بالاحترام مثل فيرتشايلد سيميكوندكتورز، ويدعى رالف ببنييت، وبدا رجل الأعمال الذي تجاوز الخمسين من عمره، من وجهة نظر الأساتذة الجامعيين الثلاثة، خياراً حسناً شأن أي خيار آخر متاح.

ولقد أخذت الشركة تجمع لديها الطاقة العاملة اللازمة، بمساعدة بينيت، وكان من بين هؤلاء شاب اختصاصي بالتسويق يدعى بارت أوبراين. وبدا أوبرايان هذا حتّى لأكاديمي مثل لين أدليمان شخصية تدعو للتقدير، علماً بأنه سبق له العمل في شركة تختص بالتقنية العالية في فلوريدا، وتدعى باراداين. كان رجلاً شديد العناية بلباسة ومبادراً قوياً في نهجه في بيع منتجات الشركة التي يعمل فيها، يراوده حلم بأن تكون له شركته الخاصة ذات يوم. وصادف أن رافق أدليمان صاحبه أوبريان ذات مرة في زيارة عمل فسحر ببراعته في الرد على

الانتقادات، التي كان هذا الزبون المتوقع يوجهها إِلىٰ منتج الشركة.

كان فريق الباحثين الثلاثة قد وجد فكرة، تنفذ الخوارزمية «رسا» على رقاقات بالغة التعقيد، فآثر أن يكون منتجه الأول برنامج يستخدم أساساً في تشفير البريد الإِلكتروني وتخزين البيانات في أجهزة الكومبيوتر الشخصية، وقد أُطلق عليه اسم: ميلسايف البريد الآمن Mailsafe، وهو نظام شيفرة يعمل بمفتاح عام ويمكن استخدامه في أكثر أجهزة الكومبيوتر الشخصي شيوعاً، مثل الكومبيوتر الشخصي من طراز آي بي إم وعائلته. فعمل أدليمان في الخوارزميات، بينما اعتنى رايفست بالتطبيق. ومع أن أدليمان لم يجد هذا العمل مثيراً من الناحية الفكرية كالبحث النظري المحض، فقد اجتذبته سيماء البرمجة التجارية حيث اكتشف حيلاً لجعل المسائل الرياضية تجري بقدر من الكفاءة أكبر من السابق.

ولقد كان هذان الجامعيان يعملان في مشروعهما في ساعات الفراغ، ولذلك وجدا برنامج ميلسيف يستغرق إنجازه وقتاً طويلاً. وكان بديهياً ألا تحقق الشركة في فترة التطوير أية عائدات، مما أدّى إِلىٰ استنفاذ المبالغ التي دفعها كيللي في عملية الاستثمار. وهكذا أخذ الوضع يزداد سوءاً. ولئن كان بوسع الشركة، من الناحية النظرية، أن تأتي بدخل من مستثمرين من خارج الشركة، أَو تحصل على سلف عن صفقات بيع التراخيص، إِلاَّ أنَّه لم يتحقَّق في إدارة رالف بينيت الكثير من هذا. وقد ذهب بعض من كانت لهم صلة بالشركة إِلىٰ أن الرجل لم يكن يدرك طبيعة آليات التكنولوجيا المعقدة، ولا كان مهيئاً على الوجه الأمثل للتبشير بالجديد في كتابة الشّيفرة. وخلاصة القول أن المشروع الفتي كان في حالة قلقة حينما اتصل بارت أوبراين بصديق قديم من باراداين، يدعى جيم بيدزوس ليسأله المساعدة في تنشيط مبيعات البرنامج رسا RSA.

ولقد بدا الأمر يومذاك كأنه أحد الاتّصالات التي يجريها المرء، لعل الحظ يسعفه فيأتي له بحل. غير أن دخول جيم بيدزوس، لم يأت بانقلاب في

مستقبل الشركة وحسب، وإنما أتى بالتغيير للتكنولوجيا ذاتها. وهكذا وجدت كتابة الشّيفرة في بيدزوس المروج الأول لها. أما آثار هذا التطور فقد امتدت من وادي سيليكون حتّى فورت ميد.

كان جيم بيدزوس المنقذ للمفتاح العام للكتابة بالشّيفرة، وجاء من حيث لا يتوقع أحد. وكان أقرب صلة له بالخوارزمية هو حساب احتمالات ألعاب النرد في ألعاب القمار والمراهنات، بالمبالغ الضخمة في أندية لاس فيجاس التي يهوى ارتيادها. وكان بيدزوس شاباً في الحادية والثلاثين من عمره، يوناني الجنسية، وقد وُلد في 20 شباط/ فبراير 1955، «في قرية صغيرة، نائية في منطقة جبلية بالقرب من الحدود الألبانية، لا يصلها بالعالم طريق، وقد يبلغ عدد سكانها السبعين نسمة تقريباً»، على نحو ما يخبرنا. أما عائلته فقديمة العهد بالمنطقة وقد سكنتها منذ أجيال بعيدة، وكان جده قد تزوج بفتاة من قرية مجاورة، باتفاق بين الأهل. فولدت له زوجه أربعة أولاد، كان بيدزوس الثاني منهم. وفي أواخر الخمسينات غادر الوالد اليونان ليقوم بما يسميه جيم بـ«الهجرة التقليدية: فلم يكن الرجل يلم بشيء من لغة أهل البلاد، ولا كانت له خبرة بمهنة أَو عمل، ولا حظي بشيء من التعليم، ولم يكن قد اكتسب مهارة من المهارات، تعينه على أمور الحياة في المهجر. وكان جُلَّ ما فعله، هو الالتحاق بجماعة من أهل القرية، كانوا قد سبقوه إِلىٰ الهجرة وأقاموا في ولاية أوهايو». وبعد سنتين انضمت إليه زوجته وأولاده، وجيم ما يزال، بعد، في الخامسة من العمر.

وسرعان ما ألف جيم بيدزوس الحياة في أمريكا. فمع أن والديه دأبا على زرع بعض القِيَم التي حملاها من بلدهما القديم، إِلاَّ أن طبيعته المتمردة، بدأت تتلاءم مع سرعة إيقاع الحياة الأمريكية ويسرها. ثم كان له أن يمضي سنوات الدراسة بسهولة بفضل ذكائه الطبيعي، وإن لم يكن بطبيعته تلميذاً مجداً دؤوباً على الدرس على نحو خاص. ولقد وصف نفسه بالمراهق المتمرد، وإن لم

يكن بالضرورة مشاغباً، إنما حرص منذ صغره على القيام بما يطلب منه بدقة وعناية. ثم انتهى به الأمر إلىٰ دخول صفوف مشاة البحرية، وبعد قضاء خدمته الإلزامية (مع أنه لم يكن مواطناً أمريكياً، بل كان يحمل جواز سفر يوناني وما يزال) انتسب إلىٰ جامعة ماريلند، حيث درس إدارة الأعمال، وشيئاً من برمجة الكومبيوتر، وزعم أنَّه كان قد كتب أحد أوائل الفيروسات «لمجرد البرهان على إمكانية ذلك». ولكنَّه بعد عامين من الدراسة الجامعية حصل على وظيفة في شركة الآي بي إم، وانقطع بعدها عن الجامعة.

وفي مطلع الثمانينات زاره أحد محترفي البحث عن المواهب، وسأله إن كان يستهويه العمل في شركة باراداين، وهي شركة مقرها فلوريدا تقوم بصنع معدات الشبكة للكومبيوترات الضخمة؟ وشرح له هذا المنقب عن المواهب، أن عمله يختص بالتسويق، ويقتضي منه امتلاك بعض المهارات الفنية لعرض منتجات الشركة للزبائن. كانت باراداين شركة ذات مكانة مرموقة، ولديها نائبان للرئيس من أشد الإداريين كفاءة وشهرة وردا إليها من آي بي إم، وعرفا بنزعتهما المحافظة التي طغت على بعض تقاليد العمل في الشركة، من الأحذية السوداء والقمصان البيضاء والياقات المنشاة، إلى بث الشعور فيك بأنَّك أتيت إثماً عظيماً، إن كنت أول من يغادر العمل ذات يوم. بيد أن بيدزوس كان قد تعلم أصول لعبة العمل في الشركات الكبيرة. بل لقد أجاد اللعبة إلىٰ حد أنه حقَّق عدة ترقيات في سلم الوظيفة آنذاك. وهناك في باراداين تعلم بيدزوس في ما تعلم فنون التبذير، فكان ينفق في إجازاته الكثير في ما يهوى، مثل سباقات الدراجات النارية، وألعاب النرد والنساء. وتجد مذكراته، التي تعود إلىٰ السبعينات حافلة بالملاحظات حول هذه المرأة أو تلك. وتراه يحيا حياة الغاوين، وهو ما يزال، بعد، في العشرينات من عمره، ويذكرك بذلك النمط من حياة العزوبية التي يعيشها هيو هيغنر (صاحب البلاي بوي).

ولقد كاد هذا الوضع يواجه خطر النهاية، على يد امرأة كان قد بدأ

مصادقتها، ووقعت في نفسه موقعاً خاصاً. ولكن هذه العلاقة سرعان ما واجهت أزمة، حين انتقل من وظيفته تلك. ذلك أن الرجل كان قد بدأ يتسرّب إِلىٰ قلبه الملل من وظيفته التي كان يشغلها في باراداين، وأخذ يضيق بأجواء القمصان البيضاء، وراحت نفسه تهفو إِلىٰ أجواء أقل تزمتاً، وتوفر المجال لقدر أعظم من حرية الحركة والمبادرة، والمجازفة والربح. ثم المغامرة والاستقلال. ولكنَّه وجد صديقته تقول له، يوم قطع الحبل السري الذي يربطه بباراداين وشرع مع بعض أصدقائه في تأسيس شركة للتسويق على نطاق عالمي، نفس تلك الكلمات التي يرتعد منها كل عازب: إما الزواج الآن وإِلاً فلا! فقد رأت أنهما إن لم يتزوجا في تلك الفترة فلسوف يختطفه مشروعه الجديد، ولن تتاح لهما الفرصة للزواج ثانية. ولكن بيدزوس، كعهده دائماً، الرجل الذي يحدِّد ما يكون أَو لا يكون، يرفض فكرة تلقّي الإنذار من أحد، فقد وجد في ذلك ما يعني الاستسلام وفق ما تمليه عليه من شروط. إذن فهو لن يرضى الزواج تحت الضغط، حتّى ولو جاء من المرأة التي يحب. وهكذا كانت النهاية.

لقد أصابت صديقته في ما قالته عن أسلوبه في الحياة، إذ أنَّها رأت في عمله الجديد، في بيع الأجهزة التقنية المعقَّدة للزبائن الأجانب، ثم ما يقدم لهم من الخدمات تبديداً للوقت. فأصبح الرجل يسافر إِلىٰ أوروبا أَو الشرق الأقصى كل شهر تقريباً، بل وكان يسافر أحياناً إِلىٰ القارتين معاً، وكأنما أصبح زلاجة على نطاق عالمي، فينزل في أفخم الفنادق ويرتاد أرقى المطاعم ويتذوَّق أغلى أنواع النبيذ، ثم يعقد الصفقة، دائماً هو صاحب الصفقة. ثم كان أن اصطدم بالجدار، وشرع يتساءل إن كان سيمضي حياته على هذا النحو، مسافراً على الدوام، باحثاً عن الزبون التالي؟ وأخذ يستعيد ذكرى علاقة الحب الذي فات. فترك الشركة وأخذ يعمل في مشاريع التسويق الحرة، كل واحدة على حدة. فإذا احتاج لبعض المال، بحث عن مشروع ونهض به حتّى ينال حاجته. وكان السأم من فلوريدا قد أخذ ينال منه حينذاك، وأراد الرحيل إِلىٰ كاليفورنيا. فتلقى

يومئذ عرضاً من شركة كان قد باعها في الماضي تلميحات موافقة للآي بي إم للعمل لديها في الساحل الغربي، لكنَّه لم يكن مهتماً بهذا العرض. ثم تابع مدير الشركة الصغيرة بعرض مضاد، إذ قال له: «أني أعلم بأنك راغب في الانتقال إِلىٰ هذه المنطقة، ثم أعلم بأنك معجب بموظفة الاستقبال لدينا. فإذا رغبت وأتيت للعمل لدينا يومين في الأسبوع، فإني مستعد لتغطية نفقات الانتقال مقابل يومين في الأسبوع، وحسبي منك ستة أشهر لا غير».

ولقد أصاب الرجل وتراً حساساً لدى بيدزوس ـ فالحقيقة، أن الفتاة وقعت موقعاً حسناً في قلبه ـ وكان أن حط رحاله في كاليفورنيا، وصادف ذلك شهر آب/ أغسطس 1985. ثم اتصل عندئذ بصديقه بات أوبراين في آر إس إيه داتا سيكيورتي.

وكان قد سبق لأوبراين أن ذكر موضوع شركة آر اس إيه لبيدزوس في أيار/ مايو، بل وحتَّى عرض عليه مشروعاً تجارياً، ولكن بيدزوس كان يتهيأ لرحلة إِلىٰ أوروبا تستغرق منه خمسة أسابيع فلم يستوعب شيئاً من الموضوع، بل ونسيه بعد ذلك في غمرة انشغاله بالسفر. فلما عاد من رحلته إِلىٰ فلوريدا وجد في شقته بضعة مغلفات في انتظاره، وجميعها تحتوي على مشاريع لـ آر اس إيه مختلفة، تنتظر الرواج؛ ويبدو أن هذه الرسائل كان لها فعل أسرع من لعبة نرد. وكان جلياً من خلال الرسائل أن هذه الشركة الجديدة الغريبة، شركة ناشئة لم تبلغ مبلغ الشركات الضخمة.

لكن بات أوبراين ظل عنيداً مثابراً وهو يحث صاحبه على العمل معه، ودعاه لمقابلته في سان فرانسيسكو في طريق عودته من رحلة كان يقوم بها إِلىٰ الشرق الأقصى. وما كاد بيدزوس يحط في سان فرانسيسكو حتَّى كان أوبراين قد بدأ فوراً رحلة عمل خاصة، تاركاً لصاحبه مفتاح شقته والسيارة ودعوة لاستضافته في الشقة لمدة أسبوع والاستمتاع بوقته هناك. ولقد أعجب بيدزوس ببغداد عند الخليج، وأخذ يكرِّر زياراته لهذه المدينة، فاستغل أوبراين هذه

المناسبات ليسأل بيدزوس النصح في قضايا التسويق والبيع، التي تتصل بالشركة. ويطلب منه الرأي في أمور لتمويل المشروع. وكان الرجل لا ينقطع عن القول لصاحبه أنه «يحسن صنعاً إن انتقل للعمل هنا».

لكن بيدزوس لم يكن مستعداً للقيام بهذه الخطوة، إنما أخذ يولي المشاريع المتصلة بشركة آر إس إيه مزيداً من وقته، فيضع خطة للتسويق مرة وينكب على دراسة احتمالات بيع المنظومة كلها للآي بي إم مرة أخرى. وكان كلما ازدادت معرفته بمنتج الشركة السحري، ازداد فضولاً ورغبة في معرفة ألغازه.

ولقد صادف ذات ليلة من ليالي أواخر عام 1985 أن التقى ألمع الشباب على الإطلاق، هويت ديفي. وحصل ذلك اللقاء حين انضم بيدزوس إِلىٰ جماعة شركة آر إس إيه، التي وجهت إِلىٰ ديفي دعوة للعشاء في المطعم المكسيكي في ضاحية ستانفورد. وكانت الشركة قد دأبت منذ حين على حثّ مخترع المفتاح العام ليكون كبير العلماء لديها (حتّى كاد ديفي أن يقبل بالعرض، غير أنه ظل يماطل في الرد بانتظار ازدياد نصيب الشركة من التمويل). وكانت المجموعة تضم أوبراين ورالف بينيت وآل ألكورن، الشخصية البارزة في أوائل عهد الأتاري والآبل؛ وكانت الشركة تحاول أن تستدرجه للانضمام إِلىٰ الشركة. ذلك أن بيدزوس وجد نفسه مسحوراً بالتفاعل والجدل اللذين كانا يطبعا العلاقة بين ألكورن الذكي العاقل وديفي ذي الفكر المراوغ. ولقد اتفق المفكران بعد مناقشة عاجلة حول آفاق الخوارزمية، وارتاح بيدزوس للمحادثة وانشرح لها واستهواه موضوعهما.

ولقد بلغ الارتياح ببيدزوس حدّاً دفعه إِلىٰ سؤال ديفي، بعد انتهاء السهرة، إن كان لديه الوقت لمشاركته الغداء ومواصلة الحديث. وكان رد ديفي أنه «مهيّأ دائماً للغداء». وقد دأب بيدزوس طوال الشهور القليلة، بل قل

السنين، التالية على اصطحاب ديفي للغداء في بالو آلتو وبيركلي، وأخذ العلم عنه في كتابة الشّيفرة والمفتاح العام والخصوصية والسياسة. وكانت محصلة تلك اللقاءات أن أصبح الرجل محيطاً بدقائق الكريبتوجرافيا. ولكن رالف بينيت لم يبد ـ بقدر ما يستطيع بيدزوس الاستدلال ـ شغفاً بديفي. كذلك كان حال ديفي. . ويذكر بيدزوس أن الثلاثة اجتمعوا على طاولة الغداء ذات يوم، وكان ديفي ينظر باشتهاء إلىٰ شطيرة من اللحم والجبنة كان يتناولها بينيت. وبدت تلك النظرة حادة حتى أن بيدزوس بدا متأكداً من أن صاحبه ديفي يوشك على الاندفاع وأخذ الشطيرة من صحن صاحبها. وأن بينيت ولا ريب لاحظ تلك النظرة، لأنه عرض على ديفي قطعة من تلك الشطيرة. ولكنه أبى، وظل يحدق فيها. وفجأة، إذا بالعالم في الكريبتوجرافيا ذي اللحية والشعر المرسل يسحب سكيناً ضخمة، ويقرب إليه الصحن الذي يحتوي على الشطيرة ويقطع نصفها، وراح يتناولها بهدوء. والله وحده يعلم حقيقة ما كان يدور في فكر بينيت. ولكن من الواضح أن تلك اللحظة، لم تكن من اللحظات التي تتوثق فيها العلاقات.

وسرعان ما أدرك بيدزوس أن هذه الشركة الصغيرة التي تحاول الترويج لمنتجع عجيب وظيفته تعمية بيانات الكومبيوتر تعاني متاعب ضخمة، إذ تفتقر للزبائن، بل هي بحاجة لإجازة الخوارزمية أيضاً. أما تكاليف التشغيل فكانت ضخمة ينوء بها أصحابها. وكان إيجار المكان وحده عبئاً ثقيلاً. فأوبراين، المتفائل دائماً، قد استأجر للشركة رقعة كبيرة في ريد وود سيتي قريباً من الخليج، مقابل ناحية أوراكل تماماً. وكانت تلك الرقعة واسعة تصلح ملعباً لكرة القدم، وإن لم يبق من الموظفين إلاّ أقل من خمسة.

وكان هناك، الآن، لغم أرضي آخر ينتظر المناسبة للانفجار.

ويتضمن الحصول على قرض من مصرف للاستثمار على رأسه شخصان

يقيمان في نيويورك. وكان أحدهما إيطالياً يدعى فيني، وما تزال لهجته تحمل آثار لغته الإيطاليّة. أما شريكه فكان يهودياً ذا نعومة وكياسة في الحديث، يدعى ستيف. وكان هذان الشخصان يؤثران عقد لقاءاتهما في مطعم ديلي كابلان في مدينة نيويورك. ومع أن هذين الشخصين كانا في أحسن حال، إلاً أن مظهرهما كان يوحي بأنّهما هاربان من رواية لإلمور ليونارد.

وكانت الشركة قد اقترضت لاستثمار خوارزمية رسا نصف مليون دولار منذ كانون أول/ ديسمبر 1985، من خمسين مستثمراً (منهم عشرات الأطباء في نيويورك والممثّل ديڤيد برينر، استناداً إلىٰ قول بيدزوس). ولكن شركة آر إس إيه داتا سيكيوريتي، التهمت هذا المال مثلما يلتهم العفريت الصغير ابن الثمانية، قطعة الحلوى في ليلة عيد. فقد تلاشى المبلغ، 500 ألف دولار، والقوم لم يقوموا، بعد، بعدّه، إذ استنفذته رواتب الموظفين والقروض وجسر من الديون لتغطية نفقات التشغيل. وخلاصة القول، أن الشركة كانت على حافة الإفلاس.

ولقد علم بيدزوس، يومئذ، أن رالف بينيت ألمح، فوق كل المشاكل، أنّه قد يقوم بتحويل أسهمه، في الشركة، وله منها نصيب عظيم، التي ينتمي إليها، وبذلك تصبح الجمعيات من حملة الأسهم الكبار في الشركة والقائمة على كتابة الشيفرة الحديثة. ومن غرائب الأمور، أن ما لم يأخذه الشركاء في الحسبان يومذاك احتمال أن تؤدي الخوارزمية رسا، بطرح شكل جديد ومنيع من كتابة الشّيفرة، في جو الاتّصالات بالكومبيوتر المتنامي، إلىٰ أن تنفر وكالة الأَمن القومي، أو استفزاز أجهزة الأمن التي ترى نفسها مهدّدة بظهور الكسب. ويصف بيدزوس الوضع كالآتي: «لقد أدرك بارت ورالف أن لوكالة الأَمن القومي اهتماماً في هكذا موضوع. غير أنّهما كانا ينظران إلىٰ الوكالة كزبون محتمل». أما من حيث إعراض وكالة الأَمن القومي الواضح عن

الاهتمام بالموضوع ـ إذ لم يصدر من وراء السياج أي سؤال أَو تهديد ـ فقد حمله ذلك على الاعتقاد، (وتبيَّن لاحقاً أن ذلك الاعتقاد كان صحيحاً) أن الأشباح (وكالة الأَمن القومي. هـ . م) وجدوا أن من الأفضل عدم التدخّل في موضوع شركة آر اس إيه. . لأن الشركة في طريقها للتداعي دون تدخّل من أحد.

يقول بيدزوس: «كان بارت تائهاً لا يدري حقيقة ما يحدث. . . والحق أنَّه رجلٌ متفائل، شديد الحماس والاندفاع. وقد حملته هذه الطبيعة على الاعتقاد بأن كل شركة كومبيوتر في العالم، ستقبل على التعاقد مع شركته، فيجني 10 ملايين دولار من كل منها. إِلاَّ أن الدلائل لم تكن لتنبئ بشيء من هذا في أي مكان». ومع ذلك، فقد وجد بيدزوس نفسه أكثر اهتماماً بالموضوع بسبب الجانب الفكري الضخم الذي يقوم عليه. وفي منتصف كانون الثاني/ يناير 1986 وافق على مرافقة أوبراين إِلىٰ بوسطن لمناقشة رايفست، في المعضلات التي تعاني منها الشركة. وكان أن طار الاثنان على متن طائرة تابعة لشركة «طيران الشعب»، وهي شركة طيران تقوم بتقديم حسومات كبيرة، ولها كل صفات شركة نقل بري تعمل على سهول تكساس. ولقد قام في الليلة السابقة للاجتماع، بمراجعة الأرقام مع أوبراين، فبدت أشد قتامة من أي وقت مضى، ولاح لهما أن حاملة لواء المفتاح العام للكريبتوجرافيا قد تذوي دون أن يقدّر لها نصب علم واحد على الأرض. ويا لها من ثورة!

في اليوم التالي وفي مكتب رايفست، وقف بيدزوس وعرض هذه الكارثة وهو يخط تفاصيل المشكلة على سبورته. . . في البداية كان سلكه مهنياً. ولكنّه حين سمع الأنباء السيئة أطلق تنهيدة وقال: «أوف، يا الله، إنني في الحقيقة كنت آمل بأن المنتج سيأتي بنتائج طيبة!» فحاول بيدزوس حمله على استيعاب الحقيقة وهي أن الإنتاج لم يلق الرواج المأمول. ففشل الخوارزمية رسا لا

يماثل عدم الفوز بشهادة أكاديمية. ذلك أن هذا الفشل تترتب عليه عواقب. وإذا أخذت من الناس مالاً كان عليك أن تتحمَّل ضرباً من المسؤولية يختلف عما تواجهه حين يتعلَّق الأمر ببحث علمي تقوم به. فلأصحاب المال حق مقاضاتك. وفي النهاية بدأ رايفست، يترنح عندما استوعب الأمر.

وما كان منهم، عندئذ، إلاَّ أن اتصلوا هاتفياً بأدليمان في جنوب كاليفورنيا. فلما سمع من أصحابه مبلغ تردي الأوضاع، استذكر الرياضي من جديد ما كان يدركه من قبل من متعة حل المشكلات النظرية في عالم الأرقام. وهكذا كان قراره بأن يجعل علاقته بالأمر نظرية: «إني مستقيل من مجلس الإدارة». ثم أنهى المكالمة.

وبعد مضي سنوات عديدة، كان أدليمان يتحدث عن دوره بحياد وتأمّل: «كنت أنا السبب إلىٰ حد بعيد في فشل الشركة. . . في البداية، لم تكن الخوارزمية (رسا) مادة محددة، كانت موجودة على الورق، وليس بالمعنى الحقيقي للوجود. ولقد التقط أحدنا الكرة، وكان في التقاطي الكرة شيء من الخير وشيء من الشر. ولو أني لم ألتقطها لكان هناك شخص آخر ليلتقط التكنولوجيا ولكانت براءة الاختراع من نصيب شخص آخر. ولكن، إن كان لي نصيب في ولادة الـ رسا، لم يكن لي ذلك النصيب الحسن في إخراج الوليد كما ينبغي، فاعتورته بعض التشوهات الخطيرة».

بعد عودة أوبراين وبيدزوس إلىٰ كاليفورنيا، قام الرجلان بتوظيف مستشار إداري مهمته محاولة العثور على مخرج من الورطة القائمة. وقد لاحظ هذا المستشار ـ مع استمرار الاجتماعات ـ الأفكار التي عرضها بيدزوس وعلَّق عليها بأنَّها مبتكرة وعملية. ثم عرض لبيدزوس فكرة جنونية زيَّنت له أن يتولَّى زمام الأمور في الشركة.

وما زال بيدزوس عاجزاً حتى اليوم عن تقديم سبب عقلاني متماسك لانضمامه للشركة وهي تعاني مأزقاً حرجاً، والتفرغ لها ليكون الأداة لإنقاذها.

بل الحق أنه ما انقطع يتساءل في أعماقه، طوال الأشهر التالية، وهو يحاول حل الأزمة مستمراً على امتداد الليالي أمام شاشة الكومبيوتر: «هل حقاً أني هنا، في هذا المكان؟ إن بوسعي أن أكون الآن جالساً على مقعد في الدرجة الأولى بإحدى الطائرات، مسافراً إلىٰ باريس لتناول «البوردو» في مطعم «تور دارجان» مع دومينيك الحلوة!» حقاً إن في هذا العمل فرصة للاستقرار في إدارة عمل ما. نعم هناك الإثارة التي تحملها التكنولوجيا الجديدة. ثم هناك إغراء الحياة في سان فرانسيسكو، نساؤها، ومطاعمها، وحفلات الحمامات الساخنة في تيبيورن. ولكن الأمر ما زال بالرغم من كل تلك الأسباب بعيداً عن المنطق. ومع أنَّه جهد ليتبين كيف يتفادى شخصياً العواقب إن دارت الأمور دورتها في دوامة التخاصم والتقاضي والمحاكم والاتهامات، فإنَّه أدرك في أعماقه بأنَّه كان يورط نفسه في ركوب قطار متهاو.

ولقد دأب فترة من الوقت يطمئن نفسه بأن دوره في هذا كله مؤقت، مجرد مساعدة الشركة للحصول على شيء من التمويل، وتوظيف مدير جديد، ثم الحصول على مكافأة ما لقاء أتعابه في هذا كله. ومن ثم، يدير الظهر ويمضي في طريقه. ولكن ما أن بلغ شهر آذار/ مارس نهايته، حتى كان جميع الموظفين قد غادروا أَو أُنهيت خدماتهم. (لم يغادر بينيت الشركة بالمعنى الفني للكلمة حتى منتصف آب/ أغسطس، بعد مفاوضات صعبة انتهت بشراء حصته، وانتهاء العلاقة المحتملة بين شركة آر إس إيه والكنيسة العلمية). وكانت تلك الجمعة الطيبة، لولا أن بيدزوس أسماها يوم الجمعة الأسود. ففي المساء ذهب للعشاء مع رايفست وبينيت، وحمل رسمياً لقب نائب المدير العام للمبيعات والتسويق. ولما كان المسؤول الرسمي الوحيد الحاضر آنذاك فقد حق له أن يسمي نفسه المدير العام.

كان شاغله الأعظم يومذاك الأزمة المالية التي أصابت الشركة. ولم يكن هناك أي مال يمكن توقع وروده، فأخذ باستدعاء الدائنين، وشرع يتفاوض

معهم. وبادرهم بيدزوس يومئذ بالقول: «عليكم الاتصال بمكتب للمحاماة. وأخبروا القوم هناك بأننا مدينون لكم بمبلغ 175 ألف دولار. ولدينا الآن 10 آلاف دولار نستطيع إعطاءها لكم على سبيل رد الدين». وردّوا عليه بأنّهم يقبلون بالأموال النقدية! وفي تلك الأثناء أخذ بيدزوس يرتّب الأمور على النحو الذي يرضي فيني وستيف. وكان للرجل، صلات حسنة بهذين الرجلين، والمثال على ذلك أنّه كان يوقع على قائمة الحساب في مطعم ديلي لكابلان، فإذا به يقترف خطأً بكتابة المبلغ المطلوب للغداء ثلاثة بدلاً من ثمانية، وهو قيمة الفاتورة. فهرعت النادلة تمطره بالشتائم، وتدعوه بالمحتال. ولقد شعر بيدزوس بالحياة تغادر جسمه. لكن فيني وستيف قابلا الموقف بابتسامة. وقالا مازحين: «لقد أعجبنا ذلك».

وبعيداً عن العاطفة والود، كان على فيني وستيف أن يفكّرا في أمر المستثمرين لديهما، فضلاً عن احتمال رفع قضية قانونية بشأن رسا، وهو احتمال وارد. وما كان منهما عندئذ سوى طلب المشورة من شخص حيادي على قدر من الاحترام، وقد أطلقا عليه اسم «حكيم وول ستريت». وكان هذا رجلاً جاداً بعيداً عن الخفّة يدخن السيجار. فلما حضر بيدزوس لمقابلته بادره بالسؤال باختصار شديد: «ما القصة؟». أخذ بيدزوس نفساً من سيجاره واندفع في حديث طويل عن العباقرة الشباب من معهد ماساتشوسيتس الذين تفتقت عبقريتهم عن طريقة للمحافظة على سرية البيانات في الكومبيوتر وتيسير أمر التجارة في القرن التالي. ولقد أعجب الساحر بما سمع، وقرر فيني وستيف الحفاظ على العهد.

كان الأمر الذي من شأنه أن ينقذ الشركة، هو إقناع الشركات الكبرى بحاجتها للكتابة بالشيفرة ثم بيعها التكنولوجيا اللازمة. في حين كان برنامج التشفير ميلسيف Mailsafe على وشك بلوغ كماله (وكان التقدير أنه سيكون جاهزاً للشحن في تموز/ يوليو)، كانت الخطة التجارية تفترض بأن الشركة لن

تبيع البرنامج جاهزاً وإنما سوف تحقِّق أرباحها من عائدات الترخيص. ولقد أعد بارت أوبراين قبل مغادرته الشركة قائمة بأسماء حوالى ثلاثين شركة ضخمة باعتبارها من الشركات المحتمل التعامل معها، فراح بيدزوس يدرس القائمة. فوجد المباحثات وشركة إيه تي آند تي AT & T، التي كان أوبراين يقدر بأنه سيفوز منها بعقد بقيمة 10 ملايين دولار متعثرة: وراح بيدزوس يتابع اللقاءات والاجتماعات مع المدراء في الآي بي إم ودي إي سي وزيروكس. ولكن المحير كان ذلك العقد الضخم الموعود الأول الذي لم يكن ليتحقق، بل كان أشبه بحورية مراوغة تلوح للناظر وهي تظهر ثم تختفي وتظل بعيدة المنال. كان الهدف الذي وضعه بيدزوس نصب عينيه هو الفوز بعقد ضخم وإلاَّ ذهبت جهوده أدراج الرياح. وها هي ذي الديون تقترب من موعد الاستحقاق، والدعاوى سوف تتلوها، وعندئذ سيكون مآل حقوق الملكية الفكرية ـ المشتراة من معهد ماساتشوسيتس ـ البيع العلني لقاء فتات، وهي درة الشركة. كان الرجل بحاجة للحصول على المال فوراً. ولكن من الذي سيكون العميل الأول؟ بل هل هناك من يهاجم ليقضم؟

وبرزت عندئذ شركة كمنقذ محتمل، شركة صغيرة للبرمجيات تدعى إيريس أسوسييتس، وهي ممولة من شركة الجداول الإلكترونية العملاقة لوتس ديفلوبمنت كوربوريشن. وكانت إيريس تختص بمنتج يدعى نوتس Notes، وهو المثال الأول لفئة جديدة من البرمجيات تدعى برامج/ عتاد المجموعات Groupware، وضعت لتستخدم من شبكة من آلاف الناس. وكانت نوتس المرشح المثالي لنظام تشفير متضمن في جهاز الكومبيوتر، نظراً لأنه يفترض بالمستخدمين تبادل كافة الرسائل بينهم إلكترونياً، حتى تلك الرسائل التي تتضمَّن الأسرار التي تحرص الشركات على سريتها أشد الحرص. وإذن، فبدون وسيلة تضمن سرية المعلومات المتبادلة وبقاءها في مأمن من تنصّت القراصنة فإنَّه من المستبعد أن يقبل عملاء لوتس ـ وهم شركات كبرى تساوي معلوماتها بلايين الدولارات ـ على شراء برامج النوتس.

وليس هناك من كان أشد إدراكاً لهذا الأمر من مخترع برنامج النوتس: راي أوزي، أحد عباقرة الكومبيوتر الخطيرين الذين لا يستطيعون شق طريقهم بالشيفرة والإفلات من ركام من الصخور ألقي بها وسط المحيط وحسب، وإنما كان صاحب رؤى أيضاً في عالم التناظر وحس غريزي بالتجارة. وكان قد بدأ حياته موظفاً في شركة داتا جنرال، وهي شركة تنتج الكومبيوتر الصغيرة، ولكنَّه حينما شاهد الميكروكومبيوتر الشخصي الذي تنتجه الآي بي إم، أدرك أن المستقبل يكمن في هذه الأدوات الشخصيَّة. وهكذا كان أن انتقل للعمل لدى إحدى أضخم الشركات التي تصنع البرمجيات لأجهزة الكومبيوتر الشخصي يومذاك، وتدعى سوفتويرارتس، وهي التي ابتكرت الجدول الإلكتروني فيزيسكالك 1. غير أن أوزي كان منشغل الفكر في سؤال يلح عليه وهو: ماذا لو أن جميع أجهزة الكومبيوتر الشخصي هذه، اتصلت ببعضها في شبكة واحدة؟ لقد رأى يومذاك أن مآل الآي بي إم الهيمنة على صناعة البرمجيات في ذلك العالم، أما الآن فالفراغ هو السائد، فراغ يأمل بأن يملأه ببرنامج من تصميمه. وكان ذلك هو برنامج نوتس Notes ولإنتاجه أسَّس شركة إيريس أسوسييتس. غير أنَّه أمضى معظم العام 1982 وهو يحاول الحصول على عقود لتمويل مشروعه، إنما دون طائل.

وفي أوائل 1983 مضى أوزي لعرض رؤاه على ميتشل كابور، مؤسِّس شركة لوتس، الذي كان قد طلع لتوه بجدول عرف باسم 3 ـ 2 ـ 1، الذي شاع استعماله بعد أن حل فور صدوره محل الفيزيسكال. وكان الشغل الشاغل لكابور يومئذ العثور على ساحر، عبقري، في كتابة البرمجيات لينفذ برنامج، السنفونية، وهو برنامج متعدد الوظائف، لتنتجه لوتس، ويجمع بين الجدول المنضد، ومعالجة النصوص وقاعدة البيانات. وهكذا كان الاتفاق: إذا استطاع تنفيذ البرنامج «السنفونية» لشركته فإن كابور يقوم بالمقابل بتمويل إيريس أسوسييتس لإنتاج البرنامج نوتس وتتولى لوتس توزيعه. وفي اليوم الذي ظهر

فيه برنامج «السنفونية» من العام 1984، قال كابور لصاحبه: «عظيم! هيا، يا راي، نفِّذ مشروعك».

كان أومي يعلم منذ حين أن الأَمن سيكون ركناً رئيساً من هيكل البرنامج نوتس، فراح يتطلع إلىٰ تطوير تقنية يستطيع بها إحباط مساعي المتنصتين والمحتالين. وكان يهوى في صغره برنامجاً تيلفزيونياً يدعى The Man From U.N.C.L.E واعتاد يومئذ تأدية دور العميل السري مع أقرانه، وهم يقلِّدون الحوادث في هذا البرنامج. فكان ذلك ما مهد لاهتمامه بالإلكترونيات فعلوم الكومبيوتر، إلاَّ أن ما أثار حماسه وحفز اهتمامه كان مقال مارتين جاردنر عن الخوارزمية رسا، سنة 1977. ولقد ذهب به الفكر إلىٰ أن برنامجه قد يفيد من نظام المفتاح العام في الشّيفرة. وكان قد وقع، بالمناسبة، في مطلع عام 1984، وهو يوشك على الانتهاء من برنامجه «السنفونية»، على مقال في مطبوعة Dr. Dobb's Journal (وهي أشبه بدليل للبرمجيات موجه للهواة) عن الترميز بواسطة الخوارزمية رسا على قاعدة الفورتران، وكان ذلك، كما يذكر، مقالاً منعشاً جداً.

غير أن الإعلان، في عام 1984، عن تطبيق الخوارزمية رسا في مجلة لهواة الكومبيوتر كان رمزاً يشير إلىٰ وضع المفتاح العام: فإن كان الإعلان المبكر عن هذا الابتكار قد أثار الكثير من الضجة في المحافل الأكاديمية إلاَّ أنَّه لم يكن هناك من يأخذ هذا المنتج جدياً كمنتج برمجي ليستخدم عملياً. بيد أن البرنامج نوتس كان يحتاج لمثل هذا المنتج. وكان أوزي قد حدَّد المشكلة، في مذكرة له عن قضايا الأمن، بما واجه منتجه من برامج المجموعات، سواء في صون السرِّيَّة، أو في التثبت من هوية المرسل والمرسل إليه:

«يود ميتش كابور بعث برسالة إلىٰ جيم مانزي [نائب الرئيس في لوتس] تتصل بموضوع معين (ولعله موضوع حسَّاس). يقوم ميتش بتوجيه الرسالة إلىٰ جيم. والسؤال أولاً هل هناك متدخل يرصد الشبكة وقام

«بتزوير» الرسالة، مع أنَّها تفيد بأن مصدرها ميتش، ثم وضعها في صندوق البريد الخاص بجيم؟ ثانياً، لقد أدرك أن الرسالة المذكورة قد مرَّت عبر عدة آلات وسيطة؛ فهل هناك من «اختلس نظرة» وعرف مضمونها وهي تسير في طريقها إِلىٰ جيم؟».

ولقد تابع أوزي وصف الطريقة التي تعالج بها، نظام الأمان التقليدي في الكومبيوتر هٰذه المشكلة، أي عن طريق سلطة مركزية توزع كلمات سر منفصلة، فأصبحت بالضرورة موزعاً مركزياً يجري عبره كل عمليات الاتصال. ولم يكن هذا النموذج يعاني من الضعف الذي ضاق منه هويت ديفي كل الضيق في أواخر الستينات، ذلك أن النظام يتداعى كله، إذا أصاب السلطة المركزية مصاب أو خطأ، أَو كشف أمرك وافتضح سرك وحسب وإنما كانت روح هذا النموذج ذاتا حبيسة عصر مقدّر له أن يطرح في ركام الخردة. كان ذلك النظام متزامن مع نموذج الإطار الكبير للحساب حيث يقوم وحش ضخم حافل بالدارات بكل حسابات معالجة الأرقام والقولبة لحساب عشرات أَو مئات المستخدمين مثل موزع أَرقام لعب آلي عملاق. ولم يكن أوزي يرى في البرنامج نوتس مجرد منتج مبتكر رائد وحسب وإنما مثالاً أصيلاً لمستقبل قوامه العمل كالشبكة، حيث تمتلك الجماهير أجهزتها الخاصة من الكومبيوتر، ولا يضطرّون للرجوع إِلىٰ أخ كبير رقمي هائل الحجم والقدرة. وكان يرى أن الاتّصالات سوف تجري، مثل نظام الهاتف، بين شخصين، مباشرة (على عكس النظام الذي عفا عليه الزمن اليوم وكانت الاتّصالات تجري فيه عبر سلطة مركزية). وقد كتب أوزي معلقاً على النموذج الذي يقوم على السلطة المركزية: إننا نعتقد بأن هذا منهج سيء. . . ذلك أنه يعيد طبيعة التوزيع التي تسم الشبكة إِلىٰ نهج «مركزية البيانات» التي كانت طابع الأجهزة الضخمة. . . كما أنَّها تبعث المشكلات التي تعتور «الحل التقليدي»، أي الثقة بأناس وآليات/ أَو بآليات غير مفهومة تماماً».

الطريق المفضل لتوفير الأمن في النهج غير المركزي، هو المفتاح العام. ولقد بدا البحث الرائد الذي وضعه ديفي وهيلمان، وكأنما يستوحي البرنامج نوتس حين وضع الإطار لمعالجة المعضلات التي عرضت لأوزي. فبواسطة «دليل هاتف عالمي» يمكن لكل شخص في المؤسَّسة أن يتصل بكل شخص آخر بواسطة مفتاحه العام. فلقد وفّر المفتاح العام طريقة يستطيع بواسطتها مستخدمو البرنامج نوتس توجيه الرسائل بسرية تامة والتأكّد من سلامة الرسالة من التزوير معاً:

«عوداً إلىٰ السيناريو السابق حيث يرسل ميتش رسالة إلىٰ جيم... ويكتب جيم مذكرة. في «نوتس» ثمة عنصر يظهر على العينة يسمى «وقّع الرسالة». البرنامج نوتس يستخدم مفتاح ميتش الخاص والرسالة ذاتها ليلحق بالرسالة الأصلية «توقيعاً» هو رمز يعرض بميتش ذاته ومحتويات الرسالة معاً. وما أن يتم توقيع الرسالة حتّى يوجه ميتش علامة «ارسل الرسالة» على العينة. وعندئذ تغادر الرسالة جهاز الكومبيوتر الخاص بميتش وتمضي عبر الشبكة وتنتهي عند الجهاز الخاص بجيم الذي يقرأها عند وصولها إليه ويتساءل إن كانت قد صدرت حقاً عن ميتش. فيطلب من العينة العنصر المسجل «تحقق من صحة الرسالة» (كان يمكن طبعاً إجراء هذه العمليّة آلياً). هنا يستعرض البرنامج نوتس الأسماء الواردة في دليل المستخدمين، للحصول على الرقم العام لميتش. وما أن يتم العثور على هذا المفتاح حتّى يستخدم البرنامج «التوقيع» الملحق بالرسالة والمفتاح العام لميتش للتحقق من صحة الرسالة. فإذا ظهرت كلمة O.K كان معنى ذلك أن الرسالة واردة فعلاً من ميتش وبصورتها الأصلية، دون أن تتعرّض للتعديل أثناء سيرها بين ميتش وجيم».

وقد خلص أوزي إلىٰ أن الخوارزمية رسا هي الطريقة الوحيدة الناجعة لتنفيذ المفتاح العام في الكريبتوجرافيا. وكان بحاجة عندئذ إلىٰ نظام متين. فلئن كان البرنامج المعروض في نشرة الدكتور دوبز Dr. Dobb's Journal ممتعاً

للهاوي إلاّ أنّه كان أبطأ من أن يصلح لبرنامج تجاري، ناهيكم عن تشفير الرسائل المطولة. فلما عزم أوزي وفريقه على الأخذ بالتشفير كان القرار قد استقر على الأخذ بنسخة مطورة من الخوارزمية رسا: وهذه منظومة مركبة تستخدم فيها طريقة المفتاح العام ليولد المستخدمون مفتاحاً متماثلاً لتشفير الرسائل في نظام تقليدي من الكتابة بالشّيفرة. وكانت حسابات الجماعة تعتمد على أن التركيبة المناسبة تقوم على الـ رسا كخوارزمية لتبادل المفاتيح ومعيار تشفير البيانات ديز، لتمويه محتوى الرسالة.

وفي تلك الفترة تقريباً تلقى ميتش رسالة غير متوقعة من رون رايفست، ويقول فيها صاحبها «لست أدري إن كنت تحتاج ما أنا بصدد عرضه، إن لدينا خوارزمية ذات فائدة تسمى رسا، ونحن نملك جميع الحقوق. . .

سأل كابور صاحبه أوزي: «هل لديك فكرة عما قيل»؟ أجاب أوزي: «آه، اللعنة. هل أصبحت رسا تخضع لنظام الإجازة؟».

وكان أن اتفق الطرفان على الاجتماع. ففي يوم 29 نيسان/ أبريل 1985، حضر بارت أوبراين ورون رايفست إلىٰ مبنى شركة إيريس. وكانت هذه بلا ريب، أهم زيارة عمل واعدة في تاريخ شركة آر إس إيه. فلما انطلق أوبراين يغني أنشودته المعهودة ويصور برقصته المألوفة أعاجيب المنظومة التي طلعت بها الشركة قاطعه أوزي قائلاً أن أصحاب إيريس مطلعون على مزايا الخوارزمية رسا ومعجبون بها. فانتقل النقاش فوراً إلىٰ البحث في الطرق التي يمكن سلوكها لتعمل الشركتان سوية. وكان أوزي متحمساً بشكل خاص أمام احتمال الاتصال برايفست دائماً للإفادة من مشورته. وكما كتب في إحدى المذكرات: «من أدرى بالخوارزمية من مبتكرها؟».

ثم تبين في سياق المباحثات أن العقبة الكأداء في قيام تعاون بين الشركتين هي المال. فلما حان الوقت للحديث بالأرقام. وكان مطلب أوبراين، في ما أسماه تقديراً أولياً، رقماً خيالياً: 100 دولار للوحدة عن الخمسة عشر ألف

عميل (أَو «مقعد») نزولاً إلىٰ 50 دولار للمقعد بعد بلوغ الرقم 100 ألف. فرد أوزي أن هذه «التقديرات بعيدة عن الواقع بعداً شديداً». وذكرهما بأن سعر الجملة لنسخة البرنامج كله لن يزيد عن مئتي دولار. ولكن أوزي وعد بأنَّه سوف يناقش موضوع السعر مع لوتس التي سوف تسدد في النهاية تكاليف التخصيص. غير أنَّه كان يعلم علم اليقين أنه لا يمكن للوتس دفع مثل هذه المبالغ.

وكان بارت أوبراين قد أشار خلال النقاش على أوزي أن يتحقَّق ما إذا كان للتشفير تأثير على مبيعات منتجات الشركة في الأسواق خارج الولايات المتّحدة. فأقر أوزي بأن الموضوع لم يخطر له ببال. فاقترح عليه كل من أوبراين ورايفست مراجعة وكالة الأَمن القومي بشأن هذه النقطة، إنما على ايريس أَو لوتس ـ أَو الشركة التي ستتولّى عملية التصدير ـ وضع استراتيجية للتعامل مع الحكومة، وقالا له: «إن هؤلاء قوم لا ينبغي الاستخفاف بهم، وعليك أن تدرك كيف يكون كسب اللعبة». ولما انتهى الاجتماع، كان أوزي قد وعى بسرعة أن هذه القضية قد تثار مهما يكن النِّظام الذي يستخدمه برنامج «نوتس»، وطلب في مذكرته أن يدرس محامو الشركة تأثير أَنظمة التصدير على المُنتَج.

ولقد انتهى اللقاء في جو من الود، إِلاَّ أن المشكلة ظلَّت على حالها: السعر الخيالي الذي تطلبه الشركة. ولكن خوارزميات المفتاح العام كانت من جهة أخرى مثالية للبرنامج «نوتس». وفي هذا يقول أوزي: «إننا نعلم من الناحية التكنولوجية ما نريد، فقد كنا قد وضعنا تصميمه وانتهى الأمر. ولكني لم أكن لأكشف أوراقي منذ الجولة الأولى، بيد أنَّهما (أوبراين ورايفست) كانا يدركان مبلغ حماسنا وهو ظاهر». إِلاَّ أن المفاوضات ظلَّت دون تقدّم فترة من الوقت. وكانت الشركة آر اس إيه تعتبر شركة لوتس واحدة من العديد من

الأهداف الهامّة المحتملة، فبدأ أوزي ما اعتبره عملية مبيعات للوتس، محاولاً إقناع الشركة بقبول أجر معقول عن الترخيص.

كان قد مرّ حوالى العام على ذلك الاتّصال بين شركة آر اس إيه وأوزي، حين انضم جيم بيدزوس إلىٰ المحادثات، دون أن يكون قد تحقّق إلاّ القليل من التقدّم. والواقع أن أصحاب برنامج «النوتس» بدأوا يشكّون بإمكانية إجازة الكتابة بالشّيفرة، بعد إجرائهم القليل من الاتّصال مع الحكومة، وحصولهم على تلميحات بأن وكالة الأَمن القومي لن تكون راضية عن برنامج ذي شأن وتكنولوجية متقدّمة مهمتها تمويه معلومات على نحو تعجز أَجهزة الكومبيوتر الضخمة في «القلعة» عن قراءتها بيسر. ولكن؛ ما أن تدخّل زعيم شركة آر اس إيه الجديد، هذا اليوناني ذو الحادية والثلاثين من العمر واللسان الطلق والذي بدا واضحاً أنَّه ليس من هواة الكومبيوتر ولا ينتمي إلىٰ مجتمع وادي سيليكون وثقافته بأي شكل ـ أدرك أصحاب ايريس أن تلك المفاوضات دخلت الآن مرحلة جديدة.

ولقد طرح بيدزوس فور انضمامه إلىٰ المحادثات، موضوع أهمية الشركة. وكان واضحاً أنَّه ينشد التوصّل إلىٰ صفقة، ولم يكن يخشى أن يوجّه المحادثة وجهة عدائية؛ فشدَّد على أصحاب لوتس أن شركته تملك التكنولوجيا التي تحتاجها شركتهم، وهي غير متوفرة لشركة أخرى؛ وبدون خوارزمية التشفير رسا لن تستخدم الشركات الضخمة بيانات «نوتس» إطلاقاً. وهكذا كان، أن أمسك جيم بيدزوس براي أوزي من مكمن الأمل، وحرص على أن يجعله يدرك ذلك. وقد استفزت هذه النزعة الهجومية أوزي وأصحابه. والحقيقة، أن أسلوب التحدي البالغ الذي أخذ به بيدزوس، كان من الحدة ما جعل القوم في إيزيس ولوتس يمضون الأسابيع وهم يتساءلون ما إذا كان هذا اليوناني اللجوج في حقيقته عميلاً للمخابرات زُرع في شركة آر اس إيه للسيطرة

على مشروع الكريبتوجرافيا. ولكن ظهور بيدزوس على المسرح، كان العامل الذي بدّد الجمود الذي بلغته المفاوضات بين الطرفين، فقد كان يجيد المناورة ويستطيع استبدال القفاز الحديدي بآخر مخملي، متى شاء. ثم عمد إِلىٰ طمأنة أصحاب ايريس أن أصحاب شركة آر إس إيه يقصد رون رايفست، وبعض الزملاء العاملين في معهد ماساتشوسيتس ـ قادرون فعلاً على مساعدتهم في وضع خوارزمية لكريبتوجرافيا ضمن برامجهم. ثم ما زاد الأمر إغراء هو أن مطالبة المالية كانت دون الأرقام الخياليَّة التي سبق أن طرحها بارت أوبراين من قبل. والواقع أن من بين انتقاداته الرئيسة التي وجّهها لأسلافه، هو الأسعار الخياليَّة التي طالبوا بها ثمناً لمنتجهم.

وكان أوزي قد أقنع المدير العام للوتس، ميتش كابور، بضرورة المفتاح العام لبرنامج «نوتس» وطالبه بالإِسراع بطرح عرض جدي. فطرحت لوتس أمام الشركة المنهكة بالمتاعب ما هي بحاجة ماسَّة إليه: تقديم سلفة عن العائدات. وكان المبلغ المطروح هو 200 ألف دولار، لكن لوتس، لن تدفع هذا المبلغ كاملاً إِلاَّ عند اكتمال عملية التطوير. غير أن بيدزوس كان سينال بموجب هذا الاتفاق 50 ألف دولار عند توقيع العقد. وكان هذا المبلغ 50 ألف دولا يمثّل في تلك اللحظة الفاصل ما بين الحياة والموت.

ولقد جرى وضع نصوص العقود في فصل الصيف، على أن يكون تنفيذها في شهر تشرين الأول/ أوكتوبر، حين يذهب جيم بيدزوس إِلىٰ مقر شركة لوتس الجديد على نهر تشارلز في ناحية كامبردج ويقوم هو وميتش كابور بتوقيع العقذ. ولكن مجموعة شركة آر إس إيه لاحظت عند وصولها إِلىٰ المقر حالة من الفوضى الشديد تعمّ المكان. وفي غرفة الانتظار تناول بيدزوس نسخة من صحيفة ذي وول ستريت جورنال، ولاحظ في الصفحة الأولى رسماً من تلك الرسوم التي اشتهرت بها الصحيفة ـ وكان لميتش كابور. أما الخبر فيفيد

بأن كابور سوف يستقيل من لوتس لمتابعة بعض مشاريعه الخاصَّة الملحَّة. وجوهر الأمر أن معلِّم اليوجا القديم قد سئم حياة التجارة التي تذهب بالروح، وهو ينشد الآن الالتحاق بعالم يسمو فوق المادة.

وقبل أن تُتاح لبيدزوس الفرصة لتقدير أثر هذا الحدث على العقد الذي ينتظر التوقيع جاءته موظفة الاستقبال، وسألته الصعود إِلىٰ الطابق الأعلى. وهناك وجد كابور، ومصدر إلهامه ما يزال يحوم في الغرفة، فبادره بالقول: «لقد قدَّمت استقالتي، وما عاد لي عمل هنا» ولكن هناك إد بيلوف، وهو الذي سيتولَّى التعامل معكم». وكان بيلوف، أحد نوَّاب الرئيس، قد سبق له العمل في إعداد الاتفاق ويتمتع بصلاحية التوقيع. وقد فعل.

وهكذا كان بوسع شركة آر إس إيه، ولديها هذا القدر من السيولة، أن تبقي أبوابها مفتوحة، والبدء بتوزيع البرنامج «ميلسيف». ولكن السؤال الذي برز هو: أي قطاع يرغب في مثل هذا الإنتاج من الكريبتوجرافيا للكومبيوتر الشخصي؟ الواقع أن أصحاب شركة آر إس إيه كانوا خلواً من كل فكرة عن هذه الناحية. فالقسم الأعظم من الجمهور الأمريكي لم يكن يعتبر ترميز البريد الإِلكتروني أمراً ملحّاً. ولكن كان هناك عدد كبير من أصحاب الهواجس، بما يتعلق وحياتهم المهنية، وهؤلاء وجدوا في المنتَج حال نزوله جاذبية، واستهواهم.

وظهر عندئذ شخص بدا أنَّه يمثِّل هذا القطاع الخفي. فمع ظهور البرنامج ميلسيف بدأت شركة آر إس إيه تتلقَّى مكالمات تبدأ بتنفس ثقيل، ثم ينطلق صاحب المكالمة بسؤال بصوت ينم عن قلقه: «ما مبلغ ضخامة المفاتيح المرافقة للميلسيف؟» ويأتي الرد: مئة وأربعون رقماً. وبعد صمت تتخلَّله أصوات التنفس يسأل المتحدث: «وما مبلغ صعوبة اكتشاف هذه الأَرقام؟» فيجيب متلقي المكالمة أن الكومبيوتر العملاق يستغرق ألف بليون سنة للعثور على المفتاح. ويسأل الرجل عندئذ وهل بوسعي الحصول على مفاتيح أضخم

حجماً؟ ويكون الجواب أجل، ثم يسمع على الخط صوت كالفحيح الشديد: «هل بوسع الحكومة تفكيك هذا المفتاح؟» فيأتي الرد بما يعني استبعاد إمكانية ذلك. ويتابع المتحدِّث أسئلته: «هل تستطيع وكالة الأَمن القومي ذلك؟». ثم يعاود الرجل الاتّصال في اليوم التالي ويكرّر الأسئلة التي سبق أن وجَّهها في اليوم السابق. وبات الرجل الذي غدا صوته مألوفاً الآن يُعرف بـ «صاحب أسئلة الشيفرة البذيء». ويقول بيدزوس: «كان واضحاً أن صاحبنا يعتقد بأننا شركة ضخمة تضيع فيها أصوات المتكلمين، بينما كنا في الحقيقة نتنادى لنصغي إليه حين يتصل بنا».

هل كانت شركة آر إس إيه تقبل بيع منتجاتها للمتحدث البذيء الذي يطلب الكتابة بالشّيفرة؟ نعم، إنها تقبل هذا البيع. فوضع الشركة، كما كانت وكالة الأَمن القومي تخشى، هو وضع أي شركة عادية تبيع منتجاتها لمن يطلبها، كائناً من كان، وذلك حقّ لها، طالما أنَّها لا تصدر منتجاتها عبر حدود الولايات المتّحدة. وهي لا تسأل الناس عن السبب الذي يحملهم على شراء منتجاتها، فهذا أمر لا شأن لأحد به، سوى الشاري ذاته. بل إن الشركة على استعداد لشحن ما تنتجه إِلىٰ صناديق البريد.

وكان بيدزوس أحياناً، يرد على مكالمات الناس حين يتصلون بالشركة. ومن هؤلاء الذين كانوا يتّصلون بالشركة شخص من بيتسبورج، وقد أطال هذا الأسئلة حول قوة المُنتَج، وخاصة ما إذا كان بوسع الحكومة تفكيك المفتاح. فسأله بيدزوس عن سبب رغبته في اقتناء البرنامج ميلسيف؟ فتبين أن الرجل يبيع أَجهزة مضادة لأَجهزة المراقبة، مثل الجهاز المستخدَم في كشف أَجهزة الاستماع الإِلكترونية التي تُزرع في الغرف والقاعات، وللتو أدرك بيدزوس أن ثمة قاسماً مشتركاً بينه وبين هذا الرجل: كلاهما يتاجر بأدوات تضعها الدولة في قائمة الأَجهزة التي تنطوي على درجة عالية من المجازفة، في تقييد فعالية أقوى للتكنولوجيا في هذا الحقل. ولقد حملت هذه المحادثة الهاتفية بيدزوس على

التساؤل أيضاً إن كان هو نفسه يخضع لمراقبة أجهزة التنصّت والاستماع السرِّيَّة.

غير أن برنامج «ميلسيف» كان مجرد استعراض هامشي؛ فلقد أدرك بيدزوس أن عائدات شركته سيكون مصدرها بشكل أساسي الشركات الكبرى التي تقبل على برنامجها وتقوم بتركيب أجهزة التشفير كجزء من منتجاتها. ولقد أخذ عدد كبير من كبار العملاء ـ ومنهم بعض من أكثر الناس نفوذاً في البلاد ـ يصطفون بانتظار حصولهم على منتجات الشركة، بعد ذلك النجاح الذي تحقّق مع إجازة الصفقة الأولى مع لوتس. فكانت شركة موتورولا في المقدمة، وكان مطلبها توفير التكنولوجيا اللازمة للمفتاح العام لتوفر الأمان لخطوط الهاتف لديها. ثم تلتها شركة ديجيتال إكويبمنت كوربوريشن ونوفيل، وكانتا تسعيان للحصول على جهاز يوفر الأمن لشبكات الكومبيوتر.

ولقد تمّت هذه الصفقات كلها بفضل مدير مبيعات الشركة الساحر: جيم بيدزوس. وعند التفاوض في أمر بيع أو تأجير الإجازات كان هو الذي يمسك بالسلاح الحاسم: براءات الملكية الفكرية. وكان قد جرى على أن يبدأ بالحديث عن طبيعة التشفير والتثبت من الهوية والتوقيع، قبل طرح سعر معين، مستفيداً في ذلك من المعلومات التي كان يستقيها عرضاً من ديفي ورايفست وأدليمان وشامير. وكان ديفي قد عزم في تلك الأثناء على ألاّ يرتبط بالعمل رسمياً مع الشركة؛ وبرّر ذلك فيما بعد بقوله: «إنني بطبيعة تكوين شخصيتي لست عصامياً، ولا كنت أقوى على عمل إلاّ إذا كان يثير اهتمامي في لحظة معينة من الزمن». أما الشركة فكانت بحاجة إلىٰ أشخاص قادرين مثل رايفست على تركيز انتباههم وكتابة آلاف السطور من رموز مُنتَج في أسابيع قلائل.

أما بيدزوس فأصبح هو ذاته شارحاً ممتازاً للثورة في كتابة الشّيفرة. فقد أصبح بعد حين يستوعب تماماً الأهمية الحاسمة، لما يسمَّى «تأثير الشبكة» Network Effect على المفتاح العام للشيفرة: ازدادت أهميته بنسبة مطردة تعادل

انتشاره بين السكان. ولذلك كان يلح دائماً على ضرورة تضمين المُنتَج الأساسي الخوارزمية (رسا)، بحيث يحصل المشتري على الشّيفرة دون أن يطلبها تحديداً.

وكان بيدزوس قد اعتاد عدم الدخول في تفاصيل الصفقة، إلاّ بعد قيامه بعرض بنية المُنتَج. وكانت الصفقات التي تطيب له هي تلك التي تضع كتابة الشّيفرة في متناول آلاف المستخدمين، أَو ربما مئات الآلاف منهم. فإذا توفرت قاعدة من الزبائن بهذا الحجم كان مطلب الشركة بضعة دولارات وحسب عن كل مقعد. وهكذا بدأ حلم بالتكوّن: عالم يستطيع فيه كل فرد أن يتواصل، وقد تواصل فعلاً، بأمان السرّيّة التي يوفرها التشفير؛ عالم لا يتبادل فيه الناس الرسائل وحسب بل يوقعون العقود ويسددون الفواتير أيضاً وبكل أسباب الوقاية المتاحة في العالم المادي. وللشركة أن تنال حصة من هذا كله. وذلكم هو حلم كل تاجر بائع. ولكنّه كان بالمقابل كابوساً لوكالة الأَمن القومي.

ظل بيدزوس لفترة طويلة من مطلع الثمانينات، في منأى عن الحكومة فلا يبلغه منها إلاّ القليل. ويقول في ذلك أنّه كانت تبلغه بين الحين والآخر شائعات تقول: أن بعض المسؤولين يحثون الوكالة بهدوء على اتخاذ إجراء ما ضد الشركة، وقد يكون له الأثر المدمّر على المؤسّسة الناشئة. وقد سمع بعضهم يقول: اشتروهم، هدّدوهم، عليكم بهم بأي حال، افعلوا ما شئتم إنما أوقفوهم! هناك مليون طريقة لذلك». ولكن لم يكن هناك من أتى بحركة في هذا السبيل. وقد ذهبت نظرية بيدزوس إلى أن الحكومة آثرت الهدوء، والانتظار حتّى تقضي الشركة على نفسها بنفسها.

أما المشككون في أوساط الحكومة، فقد أغمطوا جيم بيدزوس حقه. فما أن بلغ صيف عام 1986 نهايته حتّى كان قد أحدث في الشركة تحولاً عظيماً، وبات يتمتع بثقة الثلاثي الذي أسّس الشركة ومنحها اسمها، إن لم نقل أنه استحوذ على إعجابهم ومناصرتهم له. فبات رون رايفست صديقاً يرتبط به

برباط الود وأشد الثلاثي تأييداً له في إدارة الشركة. وكان يقابل لين أدليمان في جامعة بيركلي، فيقابله مقابلة حسنة، وإن ظلّ على شيء من التحفّظ، ومع أنّه استمر على شراكته، إلاّ أن الرجل كان كما يبدو قد سئم حياة المال والتجارة. ثم حدث أن التقى بيدزوس آدي شامير في آب/ أغسطس الذي كان قد عاد إلىٰ إسرائيل، لكنَّه توقف في منطقة الخليج في طريقه إلىٰ سانتا بربارة لحضور اجتماع الكتابة بالشّيفرة (الكريبتو) السنوي. فأمضى بيدزوس اليوم بصحبته، فوجد شامير ذكياً ألمعياً شديد النشاط فأخذ رجل الأعمال يجهد في طلب مده بالأفكار من الأخصائي بكتابة الشّيفرة الذي كان بعد كل أمر شريكاً أيضاً في كل مناسبة لدفع الشركة على طريق النجاح.

ولكن علاقة بيدزوس بمارتي هيلمان لم تكن بالعلاقة الطيبة. ففي الثمانينات حاول ديفي الذي شارك في اختراع المفتاح العام دخول عالم التجارة عن طريق بيع حلول للشيفرة تحت اسم هيلمان أسوسييتس. ولكن المشروع فشل، وربما كان السبب في ذلك تبديده الكثير من طاقته في مشاركته مع جماعة مناهضة للحرب النووية، تعرف بجماعة ما بعد الحرب. وقد شرح لاحقاً الظروف في تلك المرحلة بقوله: «لا يمكن مقارنة أهمية كتابة الشّيفرة، بالخطر الذي يتهدّد بقاء الإنسان على الأرض، وهكذا كان أن التفت للعمل في قضية بقاء الجنس البشري». ومع ذلك فقد بدا الآن متضايقاً بل منزعجاً من أن الشركة التي نهضت جزئياً بفضل أفكاره قد أخذت تشق طريقها إلىٰ النجاح، خاصة وأنّه كان على خلاف مع شركائه في النهج الذي أخذت به آر إس إيه داتا سيكيوريتي في فهم موضوع المفتاح العام. ويقول بيدزوس اليوم أنّه حاول إعادة ضم هيلمان إلىٰ الشركة ودبّر لعقد مصالحة بينه وبين الآخرين الذين أبدعوا معه المفتاح العام في إحدى الغرف في الجامعة أثناء انعقاد مؤتمر الكتابة بالشّيفرة كريبتو 86 Crypto 86 في آب/ أغسطس من ذلك العام. ويذكر بيدزوس أن هيلمان كان شديد الانفعال أثناء اللقاء وهو يرفع صوته شاكياً. لكن

الاجتماع انتهى دونما نتيجة وعمّ الجفاء ودام بين هيلمان والآخرين طوال سنوات. ويقول بيدزوس لاحقاً أنّه عرض على هيلمان أخذ نصيبٍ من أسهم الشركة «ورجاه» القبول بها، وكان قد سبق له أن أعطى ديفي مثلها أيضاً. غير أن هيلمان رفض قبول الأسهم، قائلاً أنه ليس بالرجل الذي يعرف التعامل بالأسهم. (وكان قَبِل مُرتّباً بصفته «مشاركاً ممتازاً»).

وكان الرجل سيجني، ـ لو أنّه قَبِل تلك الأسهم ـ أكثر من مليون دولار، كما كان حال ديفي. وهذا نقيض المبلغ الهزيل الذي دفعته لهما جامعة ستانفورد التي كانت تحتفظ ببراءة الملكية الفكرية عن إنجازاتهم، فلم يزد نصيب ديفي من ذلك المبلغ عن 10 آلاف دولار.

وفي مطلق الأحوال كانت شركة آر إس إيه داتا سيكيوريتي إنكوربوريتيد قد أخذت بالإقلاع، لكنها كانت في الوقت ذاته قد أعطت الإشارة لرادار وكالة الأَمن القومي. وكان أول من لاحظ ذلك زبائن الشركة.

براءات ومفاتيح

كان الأمر كله لراي أوزي مسألة بسيطة لا تستدعي من الفكر كبير عناء ليحيط بها. فهو رجل يعمل في ابتكار منتج يتبادل فيه الناس معلومات، يحرصون على حمايتها من التسرّب أو عبث العابثين. أما إدخال التشفير بين مكونات المُنتَج فما كان إلاّ وسيلة لتوفير هذه الحماية. وإذن فالمسألة عنده محض عمل وتجارة تفرضها البداهة. أما وقد أخذت شركة لوتس الآن تعد لجعل الخوارزمية رسا جزءاً أساسياً من البرنامج «نوتس»، فإن الرجل وجد نفسه غارقاً حتّى وسطه في دغل من الممنوع والمحظور في شؤون تصديره، وكأنّه أصبح بذلك شبه عدو للدولة. ولقد فزع حين اكتشف أن برنامجاً قصد به التجارة ويهدف لمساعدة الناس في أعمالهم يعتبر، في منطوق أَنظمة التصدير، سلاحاً، لا كالمسدس، أو حتّى الخنجر، وإنما سلاحاً للتدمير الشامل.

ولقد كان بوسع أوزي أن يتجنّب هذه الورطة كلها فلا يقوم بتصدير مُنتَجه. غير أن الأمر، إن أخذنا به على المستوى العملي، كان مؤداه اقتصار البيع على أمريكا، وهذا مما يرفضه العقل، لأن ذلك يختصر العائدات المتوقعة إلىٰ النصف على الأقل. إذ أن سوق البرمجيات، لأَجهزة الكومبيوتر الشخصي كانت سوقاً عالمية، وخاصة حينما يتعلّق الأمر بالشركات الكبيرة التي كانت

المستهلك الأول لبرنامج «نوتس». ولكن مثل هذه السوق، لم تكن قد وجدت، بعد، عندما وضعت أَنظمة التصدير. فلما أخذ أوزي ومحامو شركة لوتس يقومون بأبحاثهم وجدوا أن إجازات تصدير برامج الكريبتوجرافيا، لا تمنح على وجه العموم إلاَّ عندما كان المصدر (وهو عادة شركة ذات صِلات بالمؤسَّسة العسكرية) قادراً على تقديم كفالة حسن الصداقة والنية الطيبة لدى المستخدمين، وجدارتهم بالثقة. وقد عرفت هذه العملية بـ «إجازة المستخدم النهائي» End-User Certification. ولكن البرنامج «نوتس» كان سلعة لسوق شعبية فهو مجرد علبة، فيها شريط ملفوف أشبه بشريط المسجلة. أما المستخدمون فهم. . . مجرد أناس عاديين. ولقد أصاب الضيق محامي شركة لوتس حين عجزوا عن العثور على سابقة بإصدار رخصة تصدير، لبرنامج يتضمن شيفرة في تلك الظروف.

وكان على المرء، إن أراد الخوض في الأرض المليئة بالألغام السياسية، والفنية والحافلة بالأشباح، أي أرض تلك الأَنظمة والقيود، الإستعانة بمحام يعرف خفايا واشنطن وخبير في كسح الألغام. وهكذا مضت لوتس، وكلَّفت أحد هؤلاء بمتابعة المشكلة وتمهيد الطريق. وكان هذا المحامي هو ديف ورمسر، ونصيحته الأولى: المضي مباشرة إِلىٰ مصدر كل الاعتراضات: أي وكالة الأَمن القومي. حقاً أن القانون لم ينص على هذا الاتِّصال ـ فالقناة المعينة لهذا الغرض هي وزارة الخارجية ـ إِلاَّ أن ورمسر كان يعلم أنه من العبث الذي لا طائل منه أن يتقدَّم المرء بطلب الإجازة ما لم يكن يعلم، بما يجول في عقول هؤلاء القابعين وراء السياج الثلاثي، بشأن المُنتَج وأية علّة قد يجدونها فيه.

وهكذا مضى راي أوزي، في منتصف عام 1986، وبعيد شيوع خبر الصفقة مع شركة الآر إس إيه، إِلىٰ فورت ميد، بولاية ماريلند، لاستطلاع الموقف ومعرفة ما سوف يواجه. وكان برفقته يومذاك كل من ورمسر وألان إلدريج مهندس ايريس المسؤول عن مكونات الأمان في برنامج «نوتس»؛ وكان

أوزي في الثلاثين من عمره يومذاك، أي أصغر سناً من أن يكون بين الذين اكتسحتهم ثورة الستينات، ولكنَّه كبير السن بما يكفي لأن يكون ذا موقف متشكِّك إزاء العسكريين. غير أنَّه كمهندس ومبتكر مستغرق في العمل لم يكن ليدري تماماً أي أمر صادفه الآن.

كان راي أوزي يجهل، أمر رحلة مماثلة لهذه قام بها من قبله والت تكمان من شركة آر إس إيه، وهو، شأنه شأن أوزي، غريب طارئ إنما يحمل مخططاً من شأنه توسيع مجال الشَّيفرة [الإلكترونية] فتتجاوز النطاق الذي حدَّدته «القلعة» لنفسها. وكانت وكالة الأَمن القومي قد وجدت نفسها، وهي الواثقة من أن شركة مثل آي بي إم لا يمكن تحدّي طلبٍ باسم الأَمن القومي، أنها تجاوزت التحدي، إلاً أنه بدا واضحاً في السنوات التي أعقبت الموافقة على معيار تشفير البيانات أن المشكلة ظلَّت قائمة ولم تتلاش. ولما أخذ التشفير يزداد توغلاً في القطاع العام ـ ومعيار تشفير البيانات يصبح أشد شيوعاً داخل حدود الولايات المتّحدة ـ أصبحت قوى معينة في وكالة الأَمن القومي ترى الآن في الموافقة على معيار تشفير البيانات، بالرغم من التنازلات الكبيرة من جانب آي بي إم خطأ عظيماً. فمن كان يعلم أن الناس جميعاً بدءاً من مدراء الحلقة الوسطى حتَّى الجدات سوف يستخدمون حواسب قادرة على تنفيذ عمليات تشفير بالغة التعقيد؟ من العيار الثقيل؟ ولقد اعتبر البعض من أركان الوكالة أن زيارة فريق شركة لوتس قد تكون أقوى إشارة حتَّى الآن على أن كتابة الشّيفرة قد بدأت بالانتشار بين عامة الناس، وكان معنى زيارة راي أوزي لهؤلاء المعنيين في وكالة الأَمن القومي أن برابرة الشّيفرة قد بلغوا الباب.

كانت الأجواء المحيطة بفورت ميد والسياج الثلاثي من حولها، ومخفر الحرس، ثم الممر الطويل بما علق على جدرانه من صور لجنرالات مجهولين، والغرفة التي يقودونك إليها وهي غرفة عادية لا تختلف عن أي غرفة أخرى، وما فيها من مفروشات تبدو وكأنها كانت هناك منذ عهد [السيناتور جوزيف]

مكارثي، تثير أشد الضيق في النفس. وهذا ما جعل أوزي يفكِّر بأن هؤلاء القوم على قدر عظيم من السلطة وبيدهم زمام الأمور، وهم عازمون على استخدام سلطاتهم.

بدأ الاجتماع بدخول جماعة من مسؤولي الوكالة، وأخذ أحدهم، وهو على ما يبدو المسؤول المكلَّف بالقضية، يستنطق الرجال الثلاثة. (كشف هذا الموظف ـ الذي ينفر أوزي من الإفصاح عن اسمه ـ بأنه ظل يتابع تطور «نوتس» مدة تزيد عن عشر سنوات). وتتابعت الأسئلة: «ما هو هذا المُنتَج؟ متى يكون جاهزاً؟ أي نوع من الكريبتوجرافيا تأملون باستخدامها؟ ورد أوزي وجماعته بعرض أسلوبهم المركّب في التشفير: استخدام الخوارزمية (رسا) لتبادل المفتاح ومعيار تشفير البيانات لعملية التشفير ذاتها.

لكن مجرد ذكر معيار تشفير البيانات كان مبعثاً لفقدان جماعة وكالة الأَمن القومي صوابهم. فقال أحدهم: «ها إني أخبركم الآن بأنَّكم لن تتمكَّنوا من تصدير معيار تشفير البيانات، في أي ظرف من الظروف... إنكم لن تستطيعوا تصدير المعيار أبداً». بدا هذا قولاً غريباً. ألم تصادق وكالة الأَمن القومي ذاتها على معيار تشفير البيانات؟ يمنع تصديرك يا حبيبي إلىٰ أي كان يحمل في جيبه مئتي دولار. وهنا أخذ موظف الوكالة، يشرح لمستمعيه وضع معيار تشفير البيانات. إنه ليس مجرد نظام للتشفير، وإنما هو في الحقيقة قضية سياسيَّة ملتهبة تشغل «القلعة»، ولها مضامين وأبعاد يصعب على مهندس في القطاع الخاص استيعابها ولا حاجة له بذلك.

لم يكن أوزي يعلم حينئذ، أن وكالة الأَمن القومي كانت تمر بفترة ندم مبعثه موافقتها على DES معيار تشفير البيانات. بل أن الوكالة كانت في واقع الحال تقوم على مشروع خاص بها أطلقوا عليه اسم برنامج «دعم أمن الاتّصالات التجارية» Commercial COMSEC Endorsement Program الذي يؤمل منه القضاء على الشّيفرة المستندة إلىٰ لوسيفر، ويحل محله نظامٌ للشيفرة

خاص به، ويطلق عليه اسم «مشروع الغالب» Project Overtake. وقدّم السبب المبرر لذلك أن شيوع معيار تشفير البيانات «قد يحفز منظمة استخبارات معادية على شنّ هجوم واسع النطاق» يمكنها من تفكيك الشّيفرة. وكان هذا التبرير في حدّ ذاته ضرباً من المفارقة لأن وكالة الأَمن القومي ذاتها هي التي أجازت الحجم الأصغر لمفتاح الشّيفرة فجعلتها بذلك عرضة لمثل هذا الهجوم. ولكن المشكلة الحقيقيَّة لم تكن تكمن في كون معيار تشفير البيانات، ضعيفاً، وإنما في شدة إحكامه، فهو أشد إحكاماً مما ينبغي لنظام شيفرة يستخدمه جمهرة الناس. وها هو معيار تشفير البيانات يهدِّد بأن يزداد شيوعاً وبأكثر مما قدَّرت له الوكالة، وإذا ما استخدمت أَنظمة للمفتاح العام على نطاق تجاري واسع، مثل البرنامج «نوتس» معيار تشفير البيانات، فإن المشكلة ستزداد سوءاً. وهكذا أصبحت فورت ميد تنظر إِلىٰ الشيفرة كعنصر خطير يتهدَّد مهمتها العالمية. فكان الحل أن تخرج وكالة الأَمن القومي بشيفرتها الخاصة التي تسيطر عليها سيطرة تامّة.

ومع ذلك فقد كان «مشروع الغالب» مبادرة محكوماً عليها بالفشل منذ البداية، لأن الزبائن الذين تسعى إليهم في القطاع الخاص لم يقبلوا عليه، لعدة أسباب منها أن التكنولوجيا المستخدمة باهظة التكاليف ومعقَّدة. وكان هذا النظام يتألَّف من أَجهزة بحجم أشرطة الاستماع Audio cassette تركب في الكومبيوتر، بسعر يبلغ 1000 دولار لكل علبة. والأدهى من ذلك، أنه لم يكن يسمح للمصارف وسواها من المؤسَّسات المالية التي سئلت أن تساهم في هذا المشروع أن يكون لها أي قدر من السيطرة على النِّظام المستخدم. ثم أن الخوارزميات ذاتها كانت محمية داخل علب مصمّمة، على نحو لا يسمح بالعبث بها. بل إن المفاتيح ذاتها كان توليدها وتوزيعها حكراً على وكالة الأَمن القومي وحدها. وكيف يمكن للمرء أن يطمئن بأن وكالة الأَمن القومي لن تحتفظ بنسخ عن المفاتيح؟ وقد جاء الجواب على لسان ممثّل وكالة الأَمن

القومي، إذ قال بلهجة متعالية، في مقابلة نادرة في صحيفة وول ستريت جورنال: «لدينا أمور أفضل تشغلنا». ومؤدى ذلك بعبارة أخرى: لتثقوا بنا. وقد تضمن المقال عرضاً لتكتيكات وكالة الأَمن القومي في التسويق تنحو فيها نهج الستالينية الجديدة. وها هو ذا أحد مدراء المصارف يعرض زيارة عمل من النوع المألوف للترويج لمشروع الغالب: «يقف رجل من رجال وكالة الأَمن القومي ويشرع في إلقاء الأوامر: «عليكم يا شباب أن تفعلوا هذا». إنه توجيه. ولك أن تتخيل أي نجاح يمكن أن يلقى هكذا أسلوب». وكانت النتيجة أن المصارف أعرضت عن اعتماد النظام الذي تروج له الوكالة، مؤثرة الاستمرار بالعمل بمعيار تشفير البيانات.

ومع أن راي أوزي كان يجهل كل هذا، إلاَّ أنه أخذ يدرك أن تصدير الشيفرة مسألة شديدة الأهمية لهؤلاء ويأخذونها على محمل الجد. وأصبح واضحاً مع استمرار الاستجواب الودي في ظاهره أن جماعة وكالة الأَمن القومي يفتقرون للمفردات اللازمة للتعامل مع منتج مصمّم لسوق واسعة ذي مكوّن أمني قوي مثل اللوتس نوتس. ويصف أوزي حال هؤلاء الناس بأنَّهم «كانوا يتعاملون مع أناس يعرفون زبائنهم ويضمنون لهم إجازة المستخدم النهائي. أما نحن فكان علينا أن نبيِّن لهم أن صناعتنا لا تسير على هذا النحو». ولما حاول أوزي أن يسترسل في الشرح بدأ محاميه يضرب ساقه تحت الطاولة بقدمه محذِّراً إيَّاه من أن وكالة الأَمن القومي لا ترتاح لسماع مثل هذا الكلام. غير أن أوزي كان يرى في تلك اللحظة أنه من الأهمية أن يتولى الدفاع عن مكوِّن الشّيفرة في برنامج «نوتس»، على أساس أن من يستخدم المُنتَج إنما يجازف بكل تجارته ووسيلته للطمأنينة فهي الأمان الذي يكفله البرنامج وعدم افتراق الشّيفرة. ولكن هذه الحجة لم يبد أنها راقت للأشباح.

أخذ أوزي يتساءل، وهو في طريق عودته إلىٰ بوسطن، بعد ذلك الاجتماع الأول، إن كان ثمة ضير حقاً في الاقتصار في توزيع برنامج نوتس

داخل الولايات المتّحدة، وتفادي الدخول في هذه المعركة؟ بيد أنّه وجد هذا النهج بمثابة انتحار مالي، إذ ليس بوسعك أن تتنافس مع الشركات المُنتِجة الأخرى إن تجاهلت السوق العالمية.

وهكذا طلب أوزي من المحامين ترتيب اجتماع آخر، في كمبردج هذه المرة. فهل أصبح موقف وكالة الأَمن القومي أكثر ليناً؟ لقد جاءه الرد حين قال أحد ممثلي وكالة الأَمن القومي لفريق شركة لوتس: «أقول لكم على سبيل توضيح موقفنا أننا على معرفة منذ عهد طويل، بأنّكم قد ضمنتم برنامج اللوتس 1 ـ 2 ـ 3 برنامج شيفرة، وهذا يقع من وجهة نظرنا في نطاق سلطاتنا. ولو شئنا لكان بوسعنا فرض حظر على تصدير برنامج اللوتس 1 ـ 2 ـ 3».

لقد كان برنامج اللوتس 1 ـ 2 ـ 3، الجدول الإِلكتروني الذي يشكّل الجانب الأعظم من عائدات الشركة. وكان هذا البرنامج أكثر البرامج شعبية في العالم وكانت نسبة عظيمة من مبيعاته، إنما تتم خارج الولايات المتّحدة. فما هو «التشفير» الذي تشير إليه وكالة الأَمن القومي؟ لقد كان برنامج الجدول الإِلكتروني في لوتس يحتوي على إضافة كلمة سر بسيطة، تمنع تدخّل كل من لا يعرفها في البرنامج. والآن، من المستبعد أن تجرؤ حكومة الولايات المتّحدة فتفرض حظر شحن جميع البرمجيات التي تحتوي على كلمات سر إِلىٰ الخارج، وهو تصرّف كفيل بأن يؤدي إِلىٰ انهيار صناعة برمجيات الحواسب الشخصية برمتها. ومع ذلك فقد فعل التهديد فعله. فعندما نظر أوزي إِلىٰ محاميه من طرف عينه رأى على وجهه ملامح الذعر واضحة جلية.

ولقد بات واضحاً لراي أوزي، أثناء ذلك الاجتماع والاجتماعات الكثيرة التي عُقدت خلال السنوات الثلاث اللاحقة، أن كل موافقة يحصل عليها لتصدير البرنامج ستكون رهناً بإرادة الحكومة، بالغاً ما بلغت أهمية النوتس لشركته أَو حتّى للاقتصاد الأمريكي. ولكنّه كان قد ارتاح إذ علم أنه ما من

شخصٍ كلّفته وكالة الأَمن القومي، بتمثيلها في التعامل بفرض نوع الشّيفرة التي تُباع «داخل» حدود الولايات المتّحدة. (وجدير بالذكر أن فرض شرط كهذا مخالف لقانون أمن الكومبيوتر. ولكن من يدري ما هي الحدود التي يقف عندها هؤلاء القوم؟). وكان المفاوضون عن جانب الحكومة يردون على أوزي كلما ألمح إِلىٰ أن القيود المفروضة بموجب أَنظمة التصدير قد تقسر شركته على توزيع نسختين من برنامج نوتس، واحدة ذات تشفير عالي المستوى للتداول الداخلي ونسخة أخرى تمتثل للمواصفات الموضوعة للصادرات، بلا مبالاة قائلين: «ذلك خيارك وشأنك». كذلك كان يراود أوزي خاطر بأن وكالة الأَمن القومي ربما كانت تحثّ لوتس على وضع هيكل مفتاح سري يفيد منه الأشباح في تفكيك الرسائل التي يقوم نوتس بتشفيرها بسرعة. ولقد حاول ذات مرة جسّ نبض القوم لمعرفة إن كانت هذه غايتهم. فسأل جلاوذته: «ماذا تريدون بحق الجحيم؟» هل تنتظرون مني أن أقدم لكم باباً سرياً لتدخلوا منه؟» فجاء الرد فوراً: «لا، إننا لا نريد لك أن تجازف بأمن المُنتَج». فعاد أوزي يسأل: «إذن فماذا تبغون». فيبقى سؤاله معلقاً بلا جواب. ويظل هذا الوضع على حاله.

وفي النهاية حصل أوزي وفريقه، حوالى منتصف 1987، على تنازل من وكالة الأَمن القومي وأساسه أن الحكومة تجري تقييماً لقوة الشّيفرة، وتسمح بتصدير برنامج نوتس. ويتقرّر طول المفتاح في مفاوضات بين الطرفين، شرط أن تتخلّى لوتس عن معيار تشفير البيانات وتستخدم شيفرة بديلة. فعمدت لوتس إِلىٰ تكليف رون رايفست فوراً ليأتي بخوارزمية جديدة. لقد طلع رايفست بعد بضعة أسابيع من العمل المضني بشيفرته الخاصة التي تحمل الرمز RC-2، اختصاراً لـ «شيفرة رايفست رقم 2». (وكانت الأولى قد نُسقت). وكان النِّظام الذي خرج به رايفست شبيهاً بمعيار تشفير البيانات، بمعنى أنه شيفرة متكاملة تقوم على بدائل معقدة، إِلاّ أن مفتاحه، على العكس من معيار تشفير البيانات،

يقبل الإطالة والاختصار. وقد قامت شركة لوتس بدفع كافة تكاليف أعمال التطوير، إنما سمحت لشركة الآر إس إيه بالاحتفاظ بحقوق الملكية الفكرية. ثم سلم رايفست الشّيفرة، في 1987، إلىٰ وكالة الأَمن القومي؛ ولم يمض إلاَّ بعض الوقت حتّى بلغه أن عباقرة الشّيفرة وراء السياج الثلاثي نالوا تقريعاً من المسؤولين لعجزهم عن معالجتها.

وقد سأل أوزي رايفست: «كيف لك أن تعلم أن هؤلاء الجماعة لن يعبثوا بالشّيفرة لإضعافها؟».

وكان رد رايفست أن في تعليقات الحكومة وجهة نظر منطقية، ولذلك فهو مطمئن لما سيقومون به من تغييرات. وقد استغرق الأمر شهراً أو يزيد قليلاً ثم استؤنفت المفاوضات من جديد، ولكن ذلك لا يعني أن الطرفين كانا يقتربان من الاتفاق. ويصف أوزي الوضع بقوله: كان محتوى تلك الاجتماعات يزداد فقراً وشحّاً، وفي اعتقادي أن الجماعة كانوا يبدّدون الوقت تأخيراً للقرار». كان الانطباع لديه: أن ثمة صراعاً يدور داخل وكالة الأَمن القومي ذاتها، حول الأسلوب الذي ينبغي اتباعه في المفاوضات. فلم يكن الافتقار لإجازة تصدير يمثّل أزمة ذات شأن لشركة لوتس خلال العامين 1987 و1988، لأن برنامج نوتس كان أحد المشاريع الطموحة لإنتاج البرمجيات، وقد تأخر إنتاجها عدة سنوات. وإذن لم يكن موضوع التشفير هو ما يعرقل صناعة المُنتَج. ولكن في بداية عام 1989 بدت الأمور تعد بقرب إنجاز المُنتَج وتصنيعه. فبات حل مشكلة التصدير مسألة ذات أهمية.

كان الأمر الوحيد الذي تستند إليه لوتس، وتفيد منه هو ما تمتع به من دأب ومثابرة. والحقيقة، أن أوزي لم يكن لديه خيار آخر سوى أن يظل على دأبه ومثابرته. فكان كلما أشار إلىٰ احتمال طرح المنتج في أسواق الولايات المتّحدة وحدها وجد أن المختصين بالتسويق يصرّون على أن هذا الحلّ غير ذي جدوى من الناحية الماليَّة. وهكذا تابع الرجل الضغط، وكان لا ينقطع عن

طلب مزيد من الاجتماعات مع وكالة الأَمن القومي، وعمل جهده على تقديم كل ما تطلب من معلومات. وكان ما يحمله على هذا هو قطع طريق الإعتراض، حال نيله إجازة التصدير، بحجة كتمان معلومات تتصل بالنظام وأسلوب عمله. فلو وقعت على تقصير منه لوجدت ذريعة لمنع شحن البرنامج. ولذلك حرص أوزي، على أن تلبي لوتس حتّى أدق طلبات وزارة الدفاع مهما تكن عارضة.

ومع أن أوزي كان الطرف المتوسل في هذه العلاقة، إلاَّ أنه كان لديه بعض الثقل في الأمر. فقال ذات مرّة للقائمين على شؤون التصدير: «أتراكم تقولون: أن عليَّ الذهاب إِلىٰ من يمثلني في الكونغرس، لأخبره بأنَّكم تمنعونني من تصدير إنتاجي إِلىٰ الأسواق الخارجية؟ هل تراكم تدفعونني لإثارة ضجة لن تهدأ بسبب هذا الموضوع؟». حقاً أن لوتس قد لا تكون إحدى الشركات العملاقة من ذوات رؤوس الأموال، التي تُعدّ بالبلايين من الدولارات، إلاَّ أنَّها كانت مع ذلك، أكبر شركات صناعة البرمجيات في ذلك الوقت، ولم يكن من المناسب قيام بعض الأشباح الذين لا ملامح لهم، بإغلاق الباب في وجه محبوبة الصحافة الاقتصادية.

وفجأة ودون مقدمات ذاب الجليد في منتصف عام 1989. ويعتقد أوزي عن اقتناع بأن الصراع داخل وكالة الأَمن القومي انتهى أخيراً بتسوية، «بين جماعة تناصرنا وأخرى معارضة لنا»، حسب قول أوزي: «في البداية كانوا يلتقون بنا، لأن ذلك من طبيعة عملهم، ثم أنَّهم كانوا يريدون معرفة توجهاتنا، نحن الذين نعمل في صناعة الكومبيوترات الشخصية الطارئة. وأعتقد أنَّه دارت معارك داخلية طاحنة بين الطرفين، بعضهم يحبِّذ شيئاً من الشّيفرة في السوق للتخلص منّا، وبعضهم لا يريد طرح سابقة، بل يحرص على ألا يخرج إِلىٰ التداول شيء من هذا». والظاهر أن النصر كان للفريق الأول. وعندئذ طرح

عرض، شفاهة طبعاً، فالعرض المكتوب أشبه بالوعد الملزم، ومثل هذا المخلوق غير موجود في غابة سلطة التحكم بالتصدير.

هاكم العرض: يجوز لشركة لوتس، أن تصدر إلىٰ الأسواق الخارجية البرنامج نوتس مع عدة التشفير من الخوارزمية آر إس إيه وآر سي 2، بالإضافة إلىٰ مفتاح بحجم 32 بت [خانة ثنائية]. وقد اعتقدت جماعة وكالة الأَمن القومي أن في هذا العرض تنازلاً كبيراً من جانبهم. فعملهم هو تفكيك الرموز. ولذلك كان عليهم أن ينظروا في عواقب عملهم، خاصة إذا ما أطل عليهم الرئيس، وطلب هو أَو مجلس الأمن القومي حل رموز رسالة مشفَّرة ببرنامج كانوا قد أجازوا تصديره. والحق أن الحدس حملهم في البداية على إجازة مفتاح لا يزيد عن 24 بت. ولكن بعد المراجعة ودراسة الأمر مع كبار المسؤولين عن وضع سياسة وكالة الأَمن القومي، كما قال أحد ممثلي الحكومة، وجدوا أنفسهم مستعدين للمضي حتى «الميل الأخير» وإجازة ما كانت الوكالة تعتبره مفتاحاً ضخماً بصورة غير مألوفة يتألَّف من 32 بت.

ضخم بشكل غير مألوف؟ لقد شعر فريق اللوتس حينذاك بالارتياع. وكان معنى ذلك أن المفاتيح التي يختارها المرء لتشفير البيانات وكذلك لفك الشّيفرة كانت محدودة بمجال لا يزيد عن أربعة بلايين مفتاح إلاَّ قليلاً. فإن كنت لا تريد محاولة تفكيكها يدوياً فإن هذا الأمر ليس بالشيء الذي يذكر في عصر الكومبيوتر الجبارة. فمثل هذه المسألة إن اعترضت أولئك الذين يقتاتون السيليكون في قبو فورت ميد [وكالة الأَمن القومي] وطلب إليهم العثور على مفتاح للشيفرة بين أربعة بلايين لأخذهم الملل وراحوا يتثاءبون لسهولتها، وقد أقر جماعةِ وكالة الأَمن القومي في الاجتماع بأن الكومبيوتر العملاقة المتوفرة لديهم قادرة فعلاً على تحطيم مثل هذه المفاتيح في غضون يومين (وهذا تقدير بدا متواضعاً قليلاً). غير أن لصوص البيانات المحتملين، ليسوا بحاجة لكومبيوترات عملاقة فعلاً، لتفكيك شيفرة مركبة بمفتاح من 32 بت. ذلك أنَّهم

إن كانوا على قدر كاف من التصميم ولديهم ذخيرة مناسبة من الدولارات وفسحة من الوقت يبدّدونها بلا حساب فإن بوسعهم أن يتصدوا بما لديهم من قوة حسابية للمشكلة والعثور على المفتاح. وتذهب تقديرات شركة الآر إس إيه إلىٰ أنه من الممكن إنجاز هذه المهمة في غضون 60 يوماً. وقد أصرّ المسؤولون في الحكومة على أن مفتاحاً كافياً بهذا الحجم، وفترة طويلة كهذه، يوفّران عنصر الأمان اللازم وسألوا: «من تراه يتجشم العناء لتفكيك رسالة، أو عدة رسائل تجارية ويبذل لكل واحدة 60 يوماً؟».

ولقد بدا أن هذه النظرة تهمل المبدأ الموجه في التكنولوجيا المتقدمة والمعروف بقانون مور القائل: أن قوة الكومبيوتر الشخصية تتضاعف كل ثمانية عشر شهراً أَو نحو ذلك. وهذا يعني أن مدة الستين يوماً سرعان ما تتقلّص إلىٰ فترة شهر. وهكذا سوف لن يستغرق تفكيك مفتاح من 32 بت، في عام 1995، إلاّ أقل من أسبوع. بيد أن هذا كله كان بعيداً عن النقطة الجوهرية. فلئن كان حقاً أن قضاء أيام أَو أسابيع في تفكيك رسائل موجهة، وفق برنامج اللوتس نوتس، وهي في معظمها بريئة نسبياً يعتبر تبديداً للوقت، إلاّ أن بعض المعلومات التي تبثّها هذه الشركات الضخمة ذات الرساميل التي تبلغ مئات الملايين أَو البلايين من الدولارات هو ذو قيمة بلا ريب. فكيف تستطيع لوتس أن تطمئن هذه الشركات إلىٰ أن المعلومات بأمان، إذا ما اقتصر المفتاح على 32 بت؟ إنها لن تستطيع الزعم باستحالة تفكيك الشيفرة، بل ولا تستطيع حتى القول أن ذلك ضرب من الصعوبة. فمن حيث الأساس إن الوقوع على رسالة سرِّيَّة هو أمر أكثر من مزعج.

ومع ذلك فليس ثمة سبب قانوني يحول دون إنتاج لوتس لنسختين من المُنتَج: نسخة للتصدير بـ 32 بت ونسخة أخرى أشد منعة وأكثر أماناً للاستخدام داخل الولايات المتّحدة. وهذه النسخة الأخيرة تأخذ بالطول الذي تؤثره لوتس للمفتاح وهو 64 بت، وهذا أشد صعوبة في التفكيك بعدة أضعاف

من النسخة المعدّة للتصدير. (لنتذكّر أن كل بت يضاعف حجم حيز المفتاح. فالمفتاح الذي تكلف معرفته ضعف الجهد المبذول في معرفة نسخة الـ 32 بت لن يكون طوله 64 بت وإنما 33 بت فقط. وهكذا كانت النسخة المحلية، إذن، أشبه برفع صعوبة النسخة المصدّرة 32 ضعفاً، مع تغيير الإطار الزمني لتفكيك المفتاح من أيام إلىٰ حقب ومحصلة القول أن المرء ليس بحاجة لمخيلة عظيمة ليستخدم طريقة القوة الغاشمة ليفكك مفتاحاً من 32 بت. ولكن إذا أخذ المرء بقدرات الكومبيوتر سنة 1989 فإن بوسعه القول دون تعسّف، أن هجوماً كهذا على مفتاح من 64 بت هو أقرب إلىٰ المستحيل).

كانت مثالب إنتاج مفتاحين بقدرات مختلفة أمراً تنوء بحمله الجبال؛ وما التكاليف اللوجستية ـ رزمتان ومجموعتان من الأقراص، وجدولان بأسماء ومواصفات المنتجين ـ إلاّ البداية. وكان على أوزي وفريقه أن يتفقدوا النسختين ويتأكّدوا من تناسقهما في العمل. ولأن برنامج النوتس كان موجهاً لقاعدة من الزبائن تشمل في ما تشمل الشركات المتعددة الجنسية مثل شركة جنرال موتورز كان لا بد من كتابة البرمجيات على نحو يستطيع معه المستخدمون في هذه الشركات، ومنهم من يقيم في الولايات المتّحدة ومنهم من يعمل في بلدان أجنبية، من التخاطب مطمئنين إلىٰ أن مخاطباتهم تظل مأمونة من تطفل المتطفلين. وإذن فقد كان على لوتس أن تحرص على أن يعمل المنتج، على نحو يطمئن الناس، إلىٰ أن الرسالة الإلكترونية ستبلغ مقصدها سواء كان بعض المستقبلين في إسبانيا أم في كنساس. وكان على كل من يستخدم برنامج نوتس أن يحمل بالضرورة مجموعتين من المفاتيح ـ زوج من المفاتيح الدولية وزوج آخر من المفاتيح للداخل ـ (وإن لم يكن هذا ظاهراً للمستخدم). وكان تنفيذ ذلك كابوساً لمن يقوم بالبرمجة، لما فيه من جهد وعناء. ولكن ذلك أمر فرضته الرغبة في الإتقان، فلم يكن أصحاب لوتس يقبلون «بالمجازفة» بتقديم سوية متدنية من العمل، في هذا البلد»، على حد تعبير أوزي، وهكذا مضت الشركة وقامت بتنفيذ البرنامج.

كانت المشكلة الوحيدة التي لم يكن هناك من سبيل لتجاوزها هي أن القيد الذي فرضته الحكومة على المُنتَج الموجّه للتصدير جعلت هذا المُنتَج أضعف كثيراً من ابن عمه الأمريكي. إن لك أن تنظر إلىٰ هذا الأمر باعتباره مثلباً، عيباً، إنما كعيب ملازم للمُنتَج. فهل يرفضه الزبائن في الخارج لذاك السبب.

في البداية لم يعرض الزبائن هؤلاء عن المُنتَج بسبب من أن فكرة شراء مُنتَج ببرنامج تشفير هو من مكوناته، كانت من الجدة ما جعل الزبائن لا يبدون اهتماماً بمستويات الأمان. ويقول أوزي في هذا: «كنا نحاول بيع مُنتَج ذي استخدامات لم يكن [زبائننا] يدرون بها وهي جزء منه. وكان [هذا المُنتَج] يتطلب بطاقة شبكة لم يكونوا يملكونها وأداة توليف مصورة يفتقدونها. وبعد أن تمكنّا من إقناعهم بالتزود بهذه المكونات فحسب سألوا: «هل هذا مأمون؟» وكان جوابنا: «نعم، إنه مأمون؛ ولكن ليس بالقدر الذي عليه النسخة الأمريكية؛ إلاَّ أنه مأمون في مطلق الأحوال». ثم يسألون: «هل يمكن لأحد أن يتدخل أثناء التخاطب؟» ويكون ردنا: «لعلكم تستطيعون ذلك، إذا جمعتم ثلاثين أو أربعين من أجهزة الكومبيوتر الشخصي. ولكن يلزمكم لذلك برمجيات خاصة وسواها». وكان تعريف الزبائن بأننا نحاول حماية معارفهم وبياناتهم عملية تعليم وتربية. ولم يمض إلاَّ بضع سنوات حتى أخذت الأسئلة ترد إلينا عن السبب الذي يجعل النسخة العالمية دون المحلية قوة. وإهمالنا تضمين تلك النسخة معيار تشفير البيانات».

كانت لوتس تأمل أن تخفِّف الحكومة القيود التي وضعتها، وتسمح بمفاتيح أضخم، مع مرور الوقت، وذلك حين ينتبه الزبائن في الأسواق الخارجية إلىٰ ضعف النسخة لديهم من حيث نوعية الحماية، بالمقارنة مع النسخة الأمريكية. فلقد كانت المفاتيح ذات الاثنين والثلاثين بت مجرد حل وسط، أراد به أوزي دفع المُنتَج إلىٰ الخارج: «لقد رأينا أننا متى بدأنا طرح

(البرنامج) في الأسواق وبات لدينا زبائن ذوي شأن، غدونا في وضع يسمح لنا بطلب التحول إلىٰ مفاتيح من 48 بت [في نسخة التصدير]. ذلك ما كنا نسعى إلىٰ تحقيقه (وتلك كانت خطتنا لبلوغ هذا الهدف).

ولكن بدا في تلك الأثناء، أن الحكومة تدفع باتجاه مضاد. فقد اعتقدت وكالة الأَمن القومي أن النسخة المعدة للتصدير ظلَّت أشد متانة مما ينبغي، بالرغم من ضعف حجم المفتاح، بسبب عناصر معينة في التصميم، وهي تتصل بإمكانية إعادة تشفير معلومات هي في الأصل مشفَّرة، وقد حسب أوزي أن من شأن هذه النقطة أن تجعل تفكيك الرسالة في أسوأ الأحوال، أشد صعوبة بعض الشيء. واقترحت الحكومة، دون أن تبدي أسباباً لطلبها، إجراء تعديلات في التصميم بشكل يحقِّق لها الرضى. وكان أبعد تقدير ذهب إليه أوزي هو أن القضية ربما كانت تتصل على الأرجح بطريقة محللي الشّيفرة في وكالة الأَمن القومي في حل الرموز. ولكن حسم القضية استغرق، بعد، عدة شهور أخرى من المفاوضات، وانتهت بإعادة تصميم المُنتَج بشكل ملحوظ وجعل البرنامج أشد بطأً من سابقه في بعض النواحي.

ولم يسع أوزي إلاّ أن يتساءل: ما الجدوى من كل هذا؟ وهل تصدير برنامج اللوتس نوتس بمفتاح من 32 بت، قد حسن من وضع الأَمن القومي فعلاً؟

كان الصراع مع لوتس حول البرمجيات المصدرة مجرد علامة وحسب وإن على وكالة الأَمن القومي أن تنتبه وتواجه التحدي الذي تمثِّله ثورة التشفير، بعد سنوات من الهمود. فبعد نوبة الذعر الخفيفة التي حدثت في أعقاب الانطلاقات الأولى في أواخر السبعينات زين الفكر للمسؤولين في «القلعة» أن زمام الأمور ما زال بأيديهم وتحت سيطرتهم. ومع أن التسوية التي حقَّقها بوبي راي إنمان ـ وبموجبها يقدم علماء الشّيفرة أعمالهم لتنظر فيها وكالة الأَمن القومي ـ لم تكن لتخلو من الثغرات فإن نسبة عالية تستدعي الاهتمام من علماء الشّيفرة البارزين الذين يعملون مستقلين عن المؤسَّسات الرسمية كانوا يقدِّمون

أعمالهم طواعية أسوة بسواهم لتطلع عليها الوكالة. ولما كان ذلك قد تمّ بخيارهم الشخصي فإنّه بوسعهم تبرير قرارهم بالامتثال لمبادئ الحرية الأكاديمية. فضلاً عن ذلك لم يكن لدى هؤلاء الأكاديميين رغبة بالإخلال بالأمن القومي. ثم أن في مخاطبة الأشباح متعة، على نحو ما. فهذا الحوار كان ينطوي على إثارة معينة، ناهيك عن الإقرار الضمني بجدية العمل الذي ينهض به المرء. وكان رجال وكالة الأَمن القومي لا يقدمون أية اقتراحات في الغالبية العظمى، وإذا طلبوا أمراً فهو تعديل بسيط، وقد جرت القاعدة على أن يكون ذلك حين يقع الباحث على موضوع ذي صلة بالأساليب التي تنهجها وكالة الأَمن القومي في شيفراتها أَو في تحليل الشّيفرة.

وبعد، فلقد ظهر أن وكالة الأَمن القومي قد تدخلت، على الأقل مرة واحدة، لصالح أحد الباحثين. ولم يكن هذا الباحث سوى آدي شامير. فلقد كان شامير في السنوات التي تلت مغادرته لمعهد ماساتشوسيتس خصب الإنتاج على نحو استثنائي. فقد خرج وزملاء له إنطلاقاً من أفكار المفتاح العام بأفكار أخرى جديدة تتصل بالتشفير، ومنها ما كان مثيراً للعجب. وكان من بين تلك الأفكار فكرة اشترك في تطويرها مع أدليمان ورايفست وتقدم طريقة للعب «بوكر ذهني... وهي كلعبة البوكر العادي، سوى أنّها تنفذ بدون أوراق اللعب بعكس ما هو مألوف في العادي». وكان من المبتكرات الأهم التي خرج بها شامير برنامج «الشراكة الخفية». فلم يكن قد مضى إِلاً سنتان على مشاركته في اختراع خوارزمية الآر إس إيه، حين شغله ما أسماه مشكلة تبحث عن حل، كيف تشترك مع عدة أطراف في مفتاح واحد، خاصة إذا كان هؤلاء يتبادلون الشك والريبة؟ والحل الكلاسيكي في حالة كهذه هو معادل إِلكتروني لما يحدث في مستودع الصواريخ النووية: إذ يقتضي إطلاق الصاروخ تحريك عدة مفاتيح معاً وفي آن واحد، وهذا يتطلب وجود أكثر من شخص واحد لتنفيذ العملية. فهل تستطيع تكرار هذه العمليَّة في العالم الآلي؟ ولقد تبين أن ذلك ممكن، ولما

شرع شامير بإعمال فكره، خرج بفكرة المشاركة الخفية، وهي وسيلة لتعميم مفتاح للشيفرة بين عدة أشخاص. فإذا استطاع عدو الحصول على أي جزء من حصة شخص من هؤلاء الأشخاص من المفتاح (ويُعرف بـ «الظل») فلن يكون لذلك أية فائدة في محاولة معرفة المفتاح. أما تنفيذ الفكرة فكان البداية. وكان واضحاً أن النهج الذي ينبغي أن يسلكه المرء يتطلب تعاون كافة الشركاء حتى يتم تصميم المفتاح. ولقد توقف شامير عندئذ وراح يعمل الفكر قليلاً. . . وتساءل ماذا لو أن أحد هؤلاء اختفى أَو مات أَو اختطف؟ فقاده هذا التفكير إِلىٰ فكرة بناء القدرة على التحمّل بحيث إذا أعطيت مجموعة جزئية من المفاتيح مقرَّرة سلفاً يكون بوسعك معرفة السر. وقد باتت هذه الطريقة تُعرف بـ «مخطّط البداية» ولها استخدامات شتى، لا تعد ولا تحصى. فيمكن توزيع سرّ مهني مثل تركيبة مياه غازية بين عشرة أشخاص، ثم لك أن تضع مسبقاً ما تشاء من التركيبات المعقَّدة لاستعادة المفتاح. فإذا اجتمع مثلاً الأشخاص الستة الذين لا يطمئن إليهم من بين من يحملون ظلال المفاتيح فقد لا يتمكّنون من بناء المفتاح. غير أن الشخص الذي يتمتع بأعظم الثقة قد يتمكّن من بناء المفتاح مع شخصين آخرين في هذا المجمع.

وفي عام 1986 طلع شامير مع زميلين آخرين من زملائه في معهد وايزمن، بأسلوب مبتكر وواعد يُعرف بـ «نظام إثبات المعرفة الصفري». وهذا يتيح لأليس، باستخدام الدالة الحسابية وحيدة الاتجاه، [أليس هي الشخصية المفترضة. هـ. م] إثبات معرفتها رقماً معيناً (يخص عادة وثيقة تعُرف بها، مثل بطاقة الضمان الاجتماعي أَو البطاقة المصرفيّة)، دون كشف ذلك الرقم للسائل. وقد قال شامير فيما بعد أنه يستطيع بهذا الأسلوب «دخول مخزن تملكه المافيا مليون مرة متتالية، ويظلون غير قادرين مع ذلك على تقمص شخصيتي [واستخدام هذه المعلومات في شراء البضائع وسوى ذلك من النشاطات]». ولقد أدرك شامير ورفاقه المبتكرون قيمة هذا المخطط في عقد

الصفقات التجارية بالوسائط الإِلكترونية فتقدموا بطلب منحهم براءة الاختراع عن هذا الابتكار. غير أنّ مكتب حقوق الملكية الفكريَّة أفاد هؤلاء الباحثين، في أوائل 1987، أن اختراعهم هذا بات الآن بأمر من الجيش الأمريكي يُعتبر سراً من أسرار الدولة، ويعتبر تداول المعلومات عنه يلحق ضرراً بالأمن القومي». ولم يكن الأمر ليقتصر على منع العلماء الإسرائيليين من مناقشة الموضوع وحسب وإنما وجّه إليهم الطلب بتحذير أي شخص سبق له الاطلاع على البحث لأن اطلاع شخص آخر على الفكرة قد يؤدي إِلىٰ معاقبته بالسجن عامين. ولكن هذا التوجيه بدا صعب التحقق إن لم يكن مستحيلاً، نظراً لأن أصحاب البحث، قد قدَّموا الموضوع إِلىٰ عدد من الجامعات فضلاً عن عرضه أمام مؤتمر كريبتو 86 Crypto' 86، كما بعثوا بنسخة منه إِلىٰ جمعية الآلات الحاسبة لنشره في أيار/ مايو القادم. وبعد، كيف يمكن للحكومة الأمريكية أن توجّه المؤلفين، وهم ليسوا من الأمريكيين، وتملي عليهم ما يمكن لهم الحديث فيه أو لا يمكن؟

إن وكالة الأَمن القومي لم يكن لها ضلع في ذلك الأمر بالتزام السرِّيَّة، ولكنَّه سرعان ما بلغها من علماء أمريكيين، ومن صحيفة ذي نيويورك تايمز التي جاء من يبلغها بالموضوع المختلف عليه. وما أن مضى يومان حتَّى طوي الأمر بهدوء. ولكن شامير لم يعلم بإلغاء القرار إلاَّ بعد أسابيع، وبات مقتنعاً بتدّخل وكالة الأَمن القومي لصالحه. والسبب؟ تذهب سوزان لانداو الباحثة في السياسة المتعلقة بالشّيفرة، بعد حين، أن سبب تدخّل الوكالة هو رغبتها في استمرار مشروعها القديم الهادف إِلىٰ استمرار الباحثين في تقديم بحوثهم إليها للاطلاع. فإذا ساد الاعتقاد لدى الباحثين بأن طرح فكرة جيدة في مجال التشفير يؤدي إِلىٰ فرض حظر على تداولها فجأة جنح الباحثون إِلىٰ الامتناع عن تقديم بحوثهم إليها وانقطع تدفقها على الوكالة. وكما كتبت لانداو: «إنه من الأيسر معرفة أثر المنافسة لو قدَّموا لك أبحاثهم».

ومع ذلك فإنه بات جلياً، مع اقتراب عقد الثمانينات من نهايته، أن نهج العرض الطوعي قد استنفذ أغراضه. ثم جاءت نقطة الانعطاف، وهذا مما له مغزاه، مع بحث لرالف ميركل. وكان ميركل قد انتقل للعمل مع شركة زيروكس Xerox Corporation، في مركز البحوث الشهير التابع لها في بالوا آلتو PARC وكانت دراسته الأساسيّة ـ بل قل هواه الشاغل ـ تكنولوجيا الجزيئات الصغيرة Nanotechnology، وهو علم حديث يعتمد على آلات بحجم الذرة. ولكن الرجل ظل يتابع التطورات في عالم التشفير. وفي عام 1989 وضع ميركل بحثاً عرض فيه سلسلة من الخوارزميات التي من شأنها تسريع الحسابات المشفَّرة واختصار سعر التشفير. وكان هذا البحث في حدّ ذاته تهديداً لمهمة وكالة الأَمن القومي. غير أن بحث ميركل هذا كان مدعاة لقلق الوكالة بشكل خاص لتضمنه مناقشة لتكنولوجيا تصميم صندوق الاستبدال. وكان هذا الموضوع مسألة حسّاسة في دوائر «القلعة»، منذ أن كانت قضية مشروع لوسيفر.

وكان أن أرسلت شركة زيروكس البحث، إِلىٰ وكالة الأَمن القومي للاطلاع. (وكانت تراود الشركة آمال بالحصول على إجازة تصدير لمُنتَج يقوم على بحث ميركل هذا). وكالمعهود، قامت الوكالة بإحالة البحث إِلىٰ الخبراء داخل السياج الثلاثي وخارجه. ولكن المحصلة لم تكن هذه المرة تصويباً مفيداً أَو طلباً لبقاً بتعديل لغة البحث. فكان مطلب الوكالة هنا منع تداول البحث، بحجة أن مشروع ميركل ينطوي على تهديد للأمن القومي، دون أن تبدي مبرراً لهذا الاعتقاد.

ولقد وافقت زيروكس ـ الشركة التي تتمتع بعقود ضخمة لتعهدات حكومية ـ علىٰ طلب الوكالة. والمألوف في مثل هذه الحالات أن ينتهي الأمر عند هذا الحد. أما في هذه الحالة فيبدو أن أحد المكلفين بقراءة البحث من خارج الوكالة أزعجه الحظر الذي فرضته، وبلغ من الانزعاج ما حمله على تسريب البحث إِلىٰ متابع حر، وهاو للكومبيوتر وهو مليونير يدعى: جون جيلمور.

وكان لدى جيلمور سلاح لم يكن متوفراً قبل عقد من الزمن، عند بدء عملية الاطلاع المسبق على البحوث: الإنترنت. وكان من أكثر جماعات المناقشة شعبية من مستخدمي الشبكة (يوسنت Usenet) على شبكة وب العالمية واحد يدعى Sci. Crypt، وكان هذا أشبه بناد مفتوح طوال الليل وأشبه بولائم الكريبتو التي تُقام سنوياً في سانتا بربارة، وتقدم تياراً متصلاً من الأفكار الجديدة ونقداً لأفكار قديمة وأخباراً من عالم الشّيفرة والرموز. فقام جيلمور بتعميم بحث ميركل على أعضاء الحلقة، وإذا به يبلغ في لحظة واحدة القراء عبر 8000 كومبيوتر من مختلف أرجاء العالم. إن عالم الآلة، جعل نظام الاطلاع المسبق على البحوث الذي تعتمده وكالة الأَمن القومي أمراً غير ذي جدوى.

وقامت الوكالة عندئذ، بطي طلبها بعدم نشر البحث.

وحتّى البيروقراطيون في القلعة أخذوا في ذلك الوقت يعون واقعاً جديداً بدأ يتشكّل، وخلاصة الأمر أن التحديات التي تواجهها لم تكن تصدر عن بحوث أكاديمية، وإنما مصدرها السوق. وأفضل مثال على ذلك شركة برمجيات المفتاح العلني التي كانت تلفظ أنفاسها ذات يوم، ثم إذا بها تبعث من جديد على يد جيم بيدزوس.

كان جيم بيدزوس يؤدي فيما يقترب عقد التسعينات استعراضاً راقصاً معقداً، منفرداً، مع وكالة الأَمن القومي. وكان الخيال قد زيّن له الآن أن الوكالة جاهدة لزعزعته وشركته، وإن لم يكن يملك برهاناً حقيقياً على ذلك. فقد أبدى الكثير من زبائنه المحتملين، على ما ظهر يومئذ، حماساً في البداية لمُنتَج، وإذا بتلك الشركات تتوقف دون سبب واضح عن رد مكالماته. كذلك وجد الاهتمام من وكالات وهيئات حكومية بمنتجاته يتبخر. ولقد خامر بيدزوس شعور، استولى عليه حتّى نخاعه الشوكي بأن هذا الصمت ليس مرده شلل أصاب مهاراته في التسويق وإنما سببه ضغط خفي مصدره في ولاية ماريلند.

بل لقد بلغ به الاستغراب حداً جعله يعجب لطبيعة علاقته بامرأة أخذت تطلعه تلقائياً لسبب من الأسباب على معلومات لا يدري بها إلاً مطلع من داخل وكالة الأَمن القومي. وكانت تبدو له تلك المعلومات يومئذ مقبولة، إلاً أنه أخذ يتساءل فيما بعد ما إذا كانت تلك المرأة مأجورة من الوكالة لتقدم له معلومات مضلّلة. وقد قال لاحقاً: «أعتقد أن هذا الأسلوب معروف في دوائر المخابرات بـ «فخ العسل». والمفارقة في الأمر أن هناك من كان يتساءل بين الحين والآخر ما إذا كان بيدزوس ذاته عميلاً مزدوجاً، يتظاهر بالصراع مع وكالة الأَمن القومي بينما هو يسرِّب المعلومات خفية ويكشف أسرار التكنولوجيا في شركته. إلاً أن الرجل كان يعتقد جاداً في أعماق عقله أنه أكبر شوكة في القدم التي تستند إليها الوكالة في الضبط والاتّصالات.

وما أثار الفزع في جيم بيدزوس حوالى عام 1990 لم يكن وكالة الأَمن القومي، وإنما تهديد أقرب كثيراً إلىٰ عمله. وليس للحكومة ضلع فيه أيضاً، وإنما سببه براءات الملكية الفكريَّة لمفتاح الشّيفرة العام الذي كان الأساس الذي ترتكز عليه التكنولوجيا الخاصة بشركته. كانت المشكلة تتّصل بشيفرة لا تنافس منتجاتها شركة الآر إس إيه مباشرة، إلاً أن براءات الملكية الفكريَّة لديها تحمل النذير بالقضاء على الشركة.

كانت الشركة تسمى سايلينك Cylink، وتاريخها يشهد بالاستقرار والهدوء وأدعى للراحة من ركوب قطار التسلية في مدينة ملاهي الآر إس إيه. وكان الشريك في تأسيسها جيم أومورا، حائزاً على شهادة الدكتوراه من جامعة ستانفورد، ثم أصبح أستاذاً في جامعة كاليفورنيا بلوس أنجليس، حيث درس الهندسة الكهربائية. أما حقله الأساسي فهو نظرية المعلومات. وكان الرجل لا يحيط بشيء من الكريبتوجرافيا، شأنه في ذلك شأن كل من اتصل بعلم الكومبيوتر في تلك الأيام الخوالي ولم يعمل لوكالة الأَمن القومي. ولكنَّه كان يعلم بأستاذ مساعد شاب في ستانفورد ذي اهتمام بالموضوع. ويروي لنا أومورا

أنه دأب يسأله: «علام تضيع وقتك في الكريبتوجرافيا؟ إذ بدا لي أن هذا موضوع عقيم لا طائل منه». وكان من حسن حظ كريبتوجرافيا المفتاح العام أن هذا البروفسور ـ مارتي هيلمان ـ لم يأخذ بنصيحة أومورا.

ولما أخذ عقد السبعينات يقترب من نهايته كانت نظرة أومورا قد تغيَّرت وأصبح خبيراً في هذا الحقل. وقد أخذ فيما بعد يدرِّس منهاجاً في الكريبتوجرافيا ليزيد من دخله، وكان تلامذته من العاملين في الصناعة، وأكثرهم يعملون في المقاولات في مشاريع الحكومة ويسعون إِلىٰ تطوير مُنتَجات للمشاريع العسكرية. أما المنهاج الذي كان يقوم بتدريسه فيشتمل على مبادئ التشفير الأساسيَّة، ولم يقتصر على تعليمها على الولايات المتّحدة وحسب، بل في بلدان أخرى أيضاً مثل سويسرا. ويقول أومورا أنه كان حريصاً على ألاَّ تتضمن الدروس التي يلقيها على طلاّبه أية معلومات سرِّيَّة. ولم يكن هو ذاته قد اطلع على موضوعات سرِّيَّة. ولكن من الذي يعلم ما تعتبره الحكومة من المحظورات؟

بعد سنوات قليلة أخذ أومورا وصديق له يتعاطيان العمل بالشّيفرة فخرجا بمُنتَج، هو مفتاح عام في رقاقة سيليكون، مستخدمان في ذلك مبادلة المفاتيح كما عرفت عند ديڤي وهيلمان. ثم مضى إِلىٰ صديق آخر، يُدعى ليو موريس، وكان من أوائل المشاركين في شركة صن مايكروسيستم، وأخذ الاثنان يقلبان فكرة الإتجار بهذا المُنتَج على وجوهها، فوضعا مخططاً عملياً لتنفيذ المشروع، ثم شرعا بالاتّصال بأصحاب الرساميل لتمويله.

كان ذلك في عام 1984، أي في ذات الوقت الذي كانت تمر فيه شركة الآر إس إيه، بأصعب فتراتها تقريباً. كذلك لم يجد أومورا وصاحبه التمويل أمراً يسيراً، لأن «الممولين ما كانوا ليهتموا بأمن المعلومات»، على حد تعبير أومورا. ثم قيّض لخطة المشروع أن تقع بين يدي جيم سيمونز حين أحالها إليه أحدهم؛ ولم يكن سيمونز هذا رياضياً ومشتغلاً بالكريبتوجرافيا (كان أحد أوائل

الذين درسوا برنامج لوسيفر) وحسب، بل له نصيب في الاشتغال بالاستثمارات أيضاً. ولقد وافق عندما عرض عليه الأمر على مساعدة الشركة الناشئة سايلينك على الوقوف على قدميها.

كان محور اهتمام سايلينك، على العكس من الآر إس إيه، التي كان هدفها أن تشيع الشيفرة بين عامة الناس، حماية مراسلات الشركات الكبرى، وخاصة تلك التي تتولّى التعهدات الحكومية. فلم تكن سايلينك لتعنى بما تسمح أَو لا تسمح به وكالة الأَمن القومي. وقد سمي أول مُنتَج لها، وصدر إِلىٰ الأسواق في عام 1986، CIDEC-HS، (وحسبك ذلك من اسم ينضح إغراء). وكان هذا عبارة عن صندوق معدني مشحون بالرقاقات ومهمته تشفير الاتِّصالات الهاتفية داخل الشركة ذاتها، بواسطة نظام شيفرة مركب: ديڤي ـ هيلمان لتوليد المفاتيح ومعيار تشفير البيانات للتشفير. ولما كان الكثير من عملاء سايلينك من المؤسَّسات المالية المرخّص لها باستخدام كريبتوجرافيا تقوم على معيار تشفير البيانات (ومنها SWIFT سويفت المؤسَّسة الدولية للتعاملات المصرفية التي تتعامل بتريليون دولار في اليوم البطيء)، فإن سايلينك لم تتعرّض لمشاكل التصدير التي تفسد حياة شركات صناعة البرمجيات، مثل شركة لوتس. وهكذا سرعان ما تحوّلت تلك الشركة إِلىٰ مؤسَّسة رابحة.

كانت سايلينك قد مضت منذ البداية، إِلىٰ جامعة ستانفورد في طلب الإذن باستخدام براءة اختراع ديڤي ـ هيلمان. وعندما أجازت الجامعة استخدام البراءة، كانت الإِجازة في بداية الأمر غير حصرية. ويصف روبرت فوجنر، مستشار سايلينك، استقبال ستانفورد للطلب بأن «ستانفورد كانت ثملة بالسعادة» فقد وجدت أخيراً من سيستخدم براءة الاختراع فعلاً، وكان أن عقدنا صفقة جيدة جداً جداً». وكانت الآر إس إيه في منتصف الثمانينات تكافح كفاحاً شاقاً، والحق يقال، لترسي أقدامها، في حين كانت سايلينك الشركة الوحيدة، التي تحقّق أرباحاً من المفتاح العام. فكان أن نمت العلاقة مع ستانفورد

وانتعشت. ثم عرضت سايلينك بعدئذ أن تمنحها الجامعة مزيداً من الحقوق لاستخدام براءات المفتاح العام. وكانت تريد في جوهر الأمر السيطرة على كافة البراءات. فإذا أراد آخرون ابتكار وتسويق مخططات شيفرة تعتمد على المفتاح العام أصبح عليهم وفق هذا التدبير طلب حقوق الإجازة من سايلينك لا من ستانفورد كحقوق ترخيص من الباطن.

ولقد وافقت ستانفورد على هذا المطلب، بيد أن الأمر انطوى على علاقة ذات مغزى: نزاع مستمر حول حقوق الجامعة في الملكية الفكريَّة، كما حول حقوق معهد ماساتشوسيتس التي تملك براءة الخوارزمية RSA رسا. وكانت ستانفورد تعتقد بأن ما تملكه من البراءات تختص في جوهرها بالمفتاح العام نظراً لأنها جسَّدت الفكرة العامة لكريبتوجرافيا المفتاح المجزأ. فيمكن لأي شخص كان، وفق هذا المنطق، استخدام الخوارزمية رسا إذا شاء، لكن عليه أن يحوز على ترخيص براءات ستانفورد أيضاً. لكن محامي معهد ماساتشوسيتس ذهبوا إلىٰ أن الخوارزمية رسا موضوع مستقل. ولقد أطلق هذا الاختلاف حالة من التوتر بين الجامعتين استمر عدة سنوات. وكان ذاك (ومعذرة للتعبير) خلافاً هادئاً، نظراً لأنّه لم يكن في الأمر مبالغ ضخمة يومذاك.

ومع ذلك فقد رأى الجميع، أن الخلاف بين مؤسَّستين ضخمتين لم يكن لائقاً، وكان أن تم التوصل إلىٰ تسوية هذا النزاع بينهما. وقامت ستانفورد برزم كل براءات الملكية الفكرية لديها والخاصة بالمفتاح العام وأحالتها إلىٰ معهد ماساتشوسيتس، وقام المعهد بدوره بنقل تلك الحقوق لشركة الآر إس إيه داتا سيكيوريتي إنكوربوريتيد. فأزاح هذا العمل سحابة ضخمة كانت تخيم فوق هذه الشركة، التي كان نظامها يعتمد فعلاً على فكرة المفتاح التي طلع بها هويت ديڤي ومارتي هيلمان. ولم تعد برمجياتها الآن مشمولة كلياً بحماية براءة الملكية الفكرية وحسب، بل لم يعد ثمة مجال بعد هذا للحديث عن حقوق ستانفورد.

وفي حين أن هذا الترتيب كان مناسباً لشركة الآر إس إيه إلاً أنه وضع سايلينك في موقف ضعيف. فإذا أراد شخص الحصول على إجازة لاستخدام شيفرة المفتاح العام فلا بد له عندئذ من أن يتوجه إما إلىٰ سايلينك وإما إلىٰ آر إس إيه داتا سيكيوريتي، ولكن لا يستطيع الحصول على حقوق استخدام نظام المفتاح العام إلاً من شركة الآر إس إيه التي ابتكر مؤسسوها هذا النِّظام. لكن هذا لم يصبح مشكلة فوراً، لأن كل شيفرة كانت تسعى إلىٰ عملاء غير أولئك الذين تنشدهم الشركة الأخرى. وفي حين أن كلتا الشركتين كانتا تناصران المفتاح العام وعلى بُعد عشرة أميال من بعضهما فإن سايلينك كانت تتسم، وفق تعبير فوجنر، بـ «العزلة الشديدة والباطنية الشديدة. . . تركّز اهتمامها على تقنياتنا، وصنع مُنتَج جيد، وبيع ذلك المُنتَج لمجموعة محدودة، ولكن نوعية جيدة من العملاء». ومن الجهة المقابلة كانت سوق الآر إس إيه، العالم الأوسع من الحساب الشخصي وعيونها شاخصة إلىٰ سوق جماهيرية واسعة.

وكان من المحتم، أن تجد الشركتان نفسيهما في صراع محتدم. فبسبب من الطريقة التي جرت بها تجزئة براءات الملكيّة الفكريّة كان لكل شركة مصلحة في الدعوة إلىٰ طريقة معينة في معالجة برمجيات المفتاح العام، والحط من قيمة النهج الآخر. ولأن براءات الملكيَّة الفكريَّة الخاصة بمعهد ماساتشوسيتس لم تكن متاحة لسايلينك فإنَّها نشطت في الدعوة إلىٰ استخدام طريقة تبادل المفتاح التي ابتكرها ديفي وهيلمان. وكان الناس في هذا الحقل يعتقدون، أن الحل يكمن، بالمعنى العملي للكلمة، في الابتكارات المشتقة عن أبحاث جامعة ستانفورد وحدها، إذ توفر طريقة لاتفاق طرفين على مفاتيح سرِّيَّة؛ ولكنها على العكس من شركة الآر إس إيه لم تحدِّد الوسائل لتنفيذ نظام مفتاح شيفرة عام كامل وكفء غير أن سايلينك ذهبت في اعتقادها إلىٰ أن بوسع المستخدمين، أن يأتوا بكل ما جاءت به الآر إس إيه، وبذات القدر من الإتقان من الأمان للمعلومات والتثبت من الهوية وسوى ذلك، باستخدام مخترعات ديفي وهيلمان

استخداماً ذكياً وحصيفاً. وكان جيم أومورا قد كتب بحثاً في هذا، في 1987، وفي هذا يقول: «بوسعكم استخدام مبتكرات ستانفورد لتأتوا بما تأتي به الآر إس إيه. وأعتقد أن هذا أزعج جيم بيدزوس لأنَّه وجد أن تقنيته لم تعد التقنية الفريدة».

يقول فوجنر: «كان على شركة آر إس إيه، كي تنجح، أن ترفع من مستوى برمجياتها التطبيقيَّة التي كانت في الواقع، تركِّز على برمجيات معهد ماساتشوسيتس. وبالمقابل كان هناك سايلينك التي أصابت نجاحاً تجارياً واضحاً بفضل التقنية التي تصدرها جامعة ستانفورد. وإذن فالصراع قادم، أَو الاتفاق التجاري واقع لا بد متحقِّق».

ولقد وجد فوجنر نفسه ينضم إِلىٰ سايلينك بصفة مستشار، في 1989، ليتولّى معالجة هذا الموضوع. وفي اليوم التالي لتعيينه التقى جيم بيدزوس. ولم تكن لديه إِلاَّ فكرة بسيطة عما ينبغي أن يتوقع. وتساءل في خلده إن كان جيم بيدزوس الذي اكتسب سمعة كفنّان في ممارسة الضغط، في الصناعة الناشئة، سوف يظهر متصلباً؟ ولكن الرجل بدا أبعد ما يكون عن التصلّب. فقد تكلف بيدزوس أشد العناء، كما يذكر فوجنر، ليبدو لين العريكة، مسايراً، وكان يظهر في سلوكه الذهول لما حقّقته سايلينك من النجاح في تجارتها. وقال لفوجنر: إن الآر إس إيه ما تزال تجاهد، ليظل رأسها فوق سطح الماء: إذن ليس لسايلينك ما يحملها على القلق من تلك الشركة. ولكن الشركتين، كانتا من الجهة الأخرى تواجه كلتاهما معركة صعبة لإرساء التشفير على نطاق أوسع. وقال بيدزوس أن شركتيهما كانتا تعملان على نشر تقنية ليس هناك من يعطيها حقها، ولا من لديه رغبة بشرائها. ومما يزيد الطين بلة أن الشركتين الأضخم اللتين تأخذان بالمفتاح العام، كل واحدة منهما تدعو إِلىٰ تطبيق يختلف عما تدعو إليه الأخرى، فتثيران الحيرة في عقول الناس جميعاً!.

وهنا دعا بيدزوس صاحبه قائلاً: دعنا لا نتقاتل مع بعضنا البعض! ولم لا

نجمع كل البراءات ونعمل سوية، ونتفق على مفتاح عام معياري، ويكون لنا الترخيص والإِجازة؟ ولسوف نحقّق البلايين من الدولارات!

بدا ذلك كله منطقياً لفوجنر. فلم لا نضم قوانا إِلىٰ بعضها، حقاً؟ وحدَّثته نفسه أن ذلك سوف يحمل المحامين لدى ستانفورد على الارتياح، إذ لطالما أسف هؤلاء لمنحهم معهد ستانفورد حقوق الإِجازة الجزئية عن ممتلكاتها الفكرية. إن ستانفورد إنما عزلت نفسها حين جعلت شركة الآر إس إيه مقصد كل من يطلب المفتاح العام. وفي هذا يقول فوجنر إن: «النكتة الشائعة في ستانفورد هي أن الاتفاقية مع معهد ماساتشوسيتس للتكنولوجيا باتت مثالاً كلاسيكيّاً على ما ينبغي أن تتجنّبه عند إجازة براءة الملكيّة الفكريّة». ولذلك فقد بدت فكرة بيدزوس بجمع براءات الملكيّة الفكريّة في سلّة واحدة ـ مع الوعد برفع أجور تراخيص المفتاح العام ـ شديدة الإغراء لجماعة جامعة ستانفورد. فعملوا على حثّ سايلينك على الأخذ بها.

ولقد توصَّلت الشركتان والجامعتان إِلىٰ التفاهم في ما بينهم، يوم 17 تشرين أول/ أوكتوبر 1989، وهو ذات اليوم، الذي وقع فيه زلزال ضخم بقوة 7 درجات بمقياس ريختر هزّ منطقة الخليج. (وقّع العقد رسمياً في نيسان/ أبريل التالي). وبموجب هذا الاتفاق تصبح كافة براءات الملكيّة الفكريّة ملكاً لشركة جديدة تتألّف من آر إس إيه وسايلينك، وتخضع هذه المؤسَّسة الجديدة، وتسمى ببليك كي بارتنرز PKP، لإدارة مشتركة بالتساوي من الشركتين الأم. وقد تمكّن جيم بيدزوس من النجاح في مفاوضاته تلك. ونيل قسمة مناسبة من العائدات بنسبة 55 ـ 45 لصالح شركته، على أساس أن قيمة حقوق الملكيّة الفكريّة الخاصة بمعهد ماساتشوسيتس تفوق قيمة براءات الملكيّة الفكريّة الأخرى في الصفقة (كانت الآر إس إيه قد حصلت على بعض براءات الملكية من ستانفورد، بينما سايلينك محرومة من حق استخدام تقنيات الآر إس إيه). هذا في حين أن الجامعتين، لم تنالا إِلاَّ جزءاً يسيراً من العائدات المتوقعة: إذ

تبلغ حصة جامعة ستانفورد تسعة سنتات ولمعهد ماساتشوسيتس أقل من أربعة عشر سنتاً من كل دولار تناله الشركة الجديدة من استخدام حقوق الملكيَّة الفكريَّة من المرخصين الفرعيين.

ويذكر أومورا أن بيدزوس حاول بعيد تأسيس الشراكة، أن يحمل سايلينك على التخفيف من القول، بأنه من الممكن تنفيذ وظائف المفتاح العام بدون الخوارزمية رسا: «قال لي ما معناه: أما وقد أصبحنا شركاء الآن فرجائي أن تتوقَّف عن الترويج لطريقة ديفي ـ هيلمان وتدعم الخوارزمية رسا». فأجابه أومورا أن شركته سوف تستمر بالأخذ بالطريقة البديلة، ولكنَّه لا يرى سبباً ليكون ذلك مشكلة، «فلا يهم أي تقنية نستخدم. فنحن شركاء»، كما قال لبيدزوس.

ويفسّر فوجنر بقوله: «لم يكن هناك في عام 1990 من يهتم بالتقنية. ولكن ما أن مضى عامان حتى أصبحت التقنية موضع اهتمام الجميع».

في بداية الأمر كان المديران فوجنر وبيدزوس يعملان معاً على ما يرام. فكان فوجنر من الناحية الفنيَّة المدير المسؤول عن الإجازات وبيدزوس الرئيس. ولكن النِّظام الداخلي كان يفرض اتخاذ القرارات بالإجماع. وكان هذا المشروع بالنسبة لفوجنر، وهو محامٍ اختصاصي بقوانين الشركات بعيد عن الإدعاء والتفاخر، وقد ائتلف الآن مع رجل يزهو بعقد الصفقات الرابحة مثل بيدزوس، أشبه بالمغامرة الجنونيّة، عمادها مغامران مجنونان، يحاولان فرض معيار عالمي لمفتاح عام للشيفرة ـ وجني الملايين كل لشركته.

لقد بلغ فوجنر من الشغف بالفكرة ما جعله يعرض عن توقيع أي اتفاقية، إذا بدا له بأن مصالح كل من الآر إس إيه وسايلينك ما تزال على افتراق. وكان أول عمل للشركة أن توجّه كتاباً إلىٰ المؤسَّسة القومية للمعايير والتكنولوجيا NIST وهي الوكالة الحكومية التي تُعتبر المرجع الأخير الذي يقرّر المعايير التي ينبغي أن تقوم عليها الاتفاقيات والأسواق. وكان نجاح الشراكة بين الشركتين

يعتمد إِلىٰ حد بعيد على ما إذا كانت مؤسَّسة المعايير والتكنولوجيا، سوف تقبل ببراءات الملكيَّة الفكريَّة، التي باتت تحت سيطرة فوجنر وبيدزوس معاً معياراً معتمداً، والواقع أن ثمة عدة معايير كريبتوجرافية مختلفة يجب أن تخضع لموافقة المؤسَّسة: معيار للتوقيع الرقمي، وثان للتشفير وثالث لتبادل المفتاح وإلخ. . . فإذا تقرَّرت هذه المسائل أصبحت ثورة الشّيفرة جاهزة للإنطلاق. وعندئذ سوف يعلم مطورو البرمجيات جميعهم أية خوارزميات هي اللازمة للسرِّيَّة والتثبّت، وسيعمدون بعدئذ إِلىٰ إدماجها في برامجهم. كذلك سوف تتفاعل البرامج مع بعضها البعض، فإذا انطلق هذا الترتيب استطاع مستخدم برنامج اللوتس إرسال بريده المشفر إِلىٰ مستخدم وورد بيرفيكت Word Perfect ويستطيع مستخدم المايكروسوفت وورد Microsoft Word وضع توقيع رقمي على دفتر حسابه الحدسي. وهذه خطوة حاسمة لا بدّ من اجتيازها، ومؤسَّسة المعايير والتكنولوجيا تدرك هذا.

ولقد قرَّرت الحكومة أن ترسي تكنولوجيا التوقيع الرقمي، باعتباره المعيار الأول. ولكن حذار. فلقد كان لكل من سايلينك، وآر إس إيه فهمه الخاص للتوقيعات، وكل منهما قائم على مذهبه في المفتاح العام المنفصل: أهو مذهب ستانفورد أم مذهب معهد ماساتشوسيتس؟ وأي من المفهومين سوف تقدمه شركة ببليك كي بارتنرز للحكومة وترشحه رسمياً ليكون معياراً؟ وكان الجواب في جعبة جيم بيدزوس: ليكن هذا باسم آر إس إيه. أما قوم سايلينك فكانوا في شك؛ فبعد كل شيء كان هؤلاء قد اشتغلوا بتواقيع ديفي ـ هيلمان مدة تبلغ ست سنوات. وكان لدى بيدزوس حل لهذه المعضلة، فقال لشركائه: إذن لنقدم جوارزمية «رسا» للتوقيع، وحين نبلغ مشكلة معيار التحكم بالمفتاح (الطريقة التي تسمح باستيعاب بلايين وبلايين المفاتيح الرقمية التي يسمح نظام ضخم بمعالجتها)، فسوف نأخذ بطريقة ديفي ـ هيلمان. وقد وافقت جماعة سايلينك على هذا الاقتراح. وأرسلت رسالة من شركة ببليك كي بارتنرز، إِلىٰ

مؤسَّسة المعايير والتكنولوجيا، بتوقيع فوجنر يوم 20 نيسان/ أبريل، أي بعد أسبوعين فقط من تأسيس الشركة. وقد حثَّت الرسالة الوكالة على اعتماد خطة «رسا» كمعيار. وذهبت الرسالة بالقول، أن ببليك كي بارتنرز تكفل الترخيص بتواقيع «رسا» بشروط معقولة ميسّرة دونما تمييز».

لكن حين بلغ الأمر للتوقيع الرقمي فإن الحكومة بدت تحمل آراء أخرى.

وسط هذا الجدل المحتدم كان جيم بيدزوس ما يزال مهتماً ببقاء شركته عائمة. وهو يعمل الآن على الفوز، بأضخم صفقة ترخيص، عقدها حتى ذلك الحين ـ اتفاق واسع، مع أقوى شركة للبرمجيات في العالم: مايكروسوفت، الحوت الأبيض في محيط التكنولوجيا المتقدمة. فمنذ بضع سنوات، أصبح عباقرة الشركة يعون باطراد، أن زبائنهم قد يحتاجون إِلىٰ توفر عنصر الشّيفرة، في ما تنتجه مايكروسوفت. ومن مقر إدارة الشركة في ردموند، بولاية واشنطن، كان كبير الخبراء ناثان مرفولد، قد دأب منذ حين على تعميم مذكرات حول الأهمية التي سوف يحتلها عنصر التشفير في أجهزة الكومبيوتر. وكان مرفولد كثيراً ما يتوسل بذكر جدته ويضرب بها المثل؛ وكانت جدته هذه تعيش في منطقة زراعية اعتاد أهلها ترك أبواب بيوتهم مفتوحة دون قفل. ولم يكن في ذلك بأس في بيئة منعزلة قلما يطرقها غريب، إِلاَّ أن هذا لا يصلح لبيئة مدينية بأي حال. وكذلك الأمر مع الكومبيوتر، فالكومبيوترات كانت في حالة انتقال من وحدات منعزلة لا اتِّصال بينها وتقبع على طاولات المكاتب إِلىٰ عقد متصلة ببعضها بشبكة في قاعدة بنية تحتية عريضة واسعة. فلتوفير الحماية والأمان لكل شيء بدءاً من الضرائب حتى السجلات الطبية من تطفل المتطفلين، لا بد لك من التزود بأقفال؛ وقد أدرك مرفولد أن كريبتوجرافيا المفتاح العام هي الأقفال الموعودة.

كان مرفولد ما يزال طالباً على مقاعد الدراسة في الجامعة يوم نشرت

مقالة مارتين جادنر، عن الخوارزمية «رسا» في مجلة العلوم الأمريكية Scientific American، وأعجب بها حتى أنّه وصفها بـ «الرائعة»، كذلك التهم من غدا عالماً فيزيائياً في ما بعد (وقد درس على يد ستيفن هوكينج في جامعة كمبردج) بحث الخوارزمية رسا وورقة بحث ديفي ـ هيلمان التي استلهمها البحث. وبعد عقد من الزمن، وعقب شراء شركة مايكروسوفت، شركة البرمجيات التي أسّسها، أصبح مرفولد أحد الأعوان الأقرب والموثوقين من بيل جيتس. وقد أثار هذا المنصب حماسه إذ وجده فرصة للمساعدة في تعميم المفتاح العام. وكما كان الحال مع راي أوزي وشركة لوتس انتهى الرجل إِلىٰ التعامل مع الشخص الوحيد في هذا المجال: جيم بيدزوس.

كانت إجازة مايكروسوفت أمراً حاسماً لبيدزوس، لأنها سوف تجعل من تقنيته معياراً أمنياً لمئات الملايين من العملاء، الذين يستخدمون برامج مايكروسوفت دوس DOS ويندوز Windows وتطبيقاتهما مثل معالج الكلمات وورد Word وجدول البيانات اكسل Excel. ومع ذلك فقد دخل بيدزوس المفاوضات بروحه الهجوميّة المألوفة، متفاخراً بأنّه، باعتباره يحمل الملكيَّة الفكريَّة للاختراع، فهو المرجع الوحيد لكل من يُعنى بالشّيفرة والتشفير. ولكن هذا الادعاء والتفاخر لم يستفزا مرفولد. فإذا كانت الخوارزمية «رسا» على هذا القدر من العظمة فلم لا نجد الناس يقبلون على استخدامها؟ ولكنه سلّم بأنه سيكون من المحتم أن تشيع أنظمة المفتاح العام، ثم مازح بيدزوس بقوله: إن الناس ربما اقبلوا على استخدام هذه الأَنظمة في نهاية القرن، حين يكون أمد براءة الملكيَّة الفكريَّة قد مضى وانقضى.

غير أن هذه الملاحظة، لم تنل من متانة أعصاب بيدزوس، فاستمرت المفاوضات ـ بين رجلين كلاهما ذو شخصية ضخمة، ويرمي في المعركة أقصى ما لديه. وكانت القضايا المطروحة معقَّدة، بسبب رغبة مايكروسوفت في التمتع بحق تعديل رمز عدة تشفير الخوارزمية «رسا» ليلائم منتجاتها. ثم كان

هناك كما علم راي أوزي من قبل، عقبة أضخم تواجههم جميعاً: قوانين التصدير.

بدأت مايكروسوفت، إدراكاً منها، بأن تضمين منتجاتها عنصر التشفير يشكِّل معضلة، حواراً مع وكالة الأَمن القومي. وبالرغم من أن العلاقة الجديدة اتّسمت بالودّ، إلاَّ أنَّها لم تكن بالميسّرة. ففي الزيارات القليلة الأولى التي قام بها ممثِّلو فورت ميد إلىٰ مقر الشركة في ردموند لم يشأ هؤلاء حتى أن يكشفوا عن اسم الكنية عند مكتب الاستقبال؛ فكان على مرفولد، أن ينزل إلىٰ موظف الاستقبال ليمنحهم بطاقات الدخول دون أن تحمل أسماءهم كاملة، بل الاسم الأول وحسب. ويصف مرفولد سلوك الجماعة، بلهجة تجمع بين الاستطراف والضيق بأنَّهم «ذوو غريزة استسرارية». والأدهى من ذلك أنَّهم ما كانوا يصرحون بما هو مسموح، وما هو ممنوع. ولكنَّهم كانوا غاية في البيان في أمر واحد: آر إس إيه داتا سيكيوريتي. فيبدو أنَّهم كانوا يحملون ضغينة تجاه هذه الشركة.

وغني عن القول، أن جماعة وكالة الأَمن القومي لم يكونوا ليرتاحوا، لتولي هذه الشركة الحديثة العهد عمليَّة توفير درع مضاد لاعتراض المعترضين، والراصدين لمئات الملايين من زبائن مايكروسوفت. ولقد حاولوا تأليب مرفولد، كما يروي هو تطور الحوار، على جيم بيدزوس وشركته. وكان نهجهم في تأليبه على بيدزوس طريفاً. فبدأوا بالتلميح، دون التصريح، بأن الشّيفرة التي طلع بها رايفست وشامير وأدليمان قد تم تفكيكها خلف السياج الثلاثي. وخشي مرفولد من ألا يتمكّن من توفير قدر معقول من الأمن لزبائنه ـ فإذا كانت الحكومة تستطيع تفكيك الشّيفرة، لم لا يستطيع نصَّاب أيضاً من تفكيكها؟ ـ وهكذا أخذ يقلب بيدزوس، على مشواة زعم وكالة الأَمن القومي.

ولقد ذهل بيدزوس للمفاجأة، إذ كان يشعر بأن الصفقة في طريقها إلىٰ الاختتام. فهب لدحض هذه الادعاءات، وتابع: «لقد اتصلنا بكل منظِّر في علم

الأَرقام، وكل رياضي، وكل باحث نعرفه في هذا الحقل، ثم عادوا إلينا جميعاً، في غضون أربع وعشرين ساعة. لقد أفحمنا [مايكروسوفت] بما فعلنا، وقالوا لنا: «من الواضح أن هذا الزعم غير صحيح».

ولكن مرفولد يذكر الحادثة على نحو مختلف، فيقول ألاّ ضرورة لدحض الزعم، إذ كان يعتقد على الدوام بسلامة مبدأ الخوارزمية «رسا». إلاّ أنه يذكر أنّه كان يمازح بيدزوس، حين قال ذات مرة أن ليس ثمة طريقة تصمد أمام تحليل الشّيفرة إلاّ إذا كان ورقة الحل لمرة واحدة One-Time Pad. وكان ردّ بيدزوس منطقياً إذ قال: إن بوسع المرء الوثوق بشيفرة مطبوعة ومتاحة للناس ـ وللنقد من أي شخص في المجتمع ـ أكثر من أية خوارزمية سرِّيَّة لدى وكالة الأَمن القومي. ذلك أن مستقبل الخوارزمية «رسا» يعتمد كلياً على قوة رموزها، ولذلك فلديها كل حافز للتأكّد من قوة هذه الرموز. وفي هذا يقول بيدزوس: «إذا تمكّن أحد من تفكيك الخوارزمية فلن يكون لديك إلاّ أطلال من شركة، كان لها موقع في الصناعة ذات يوم مضى». ولكن بيدزوس تمكّن من إقناع مرفولد بوجهة نظره. وكان نفور وكالة الأَمن القومي من الخوارزمية «رسا» بالنسبة لمرفولد بمثابة شهادة لصالحها، فتساءل في خلده: لماذا تريد الوكالة منع نشرها إلىٰ هذا الحد، إلاّ إذا كان يصعب تفكيكها؟

لكن وكالة الأَمن القومي، لم تكن قد فرغت من أمرها بعد. فقد قامت بمحاولة أخرى بعد ذلك، لتثبيط عزيمة مايكروسوفت عن إجازة الخوارزمية «رسا» فأخذت بالتدقيق حول حق الشركة بالملكيَّة الفكريَّة للخوارزمية. وراح جماعة الوكالة يشكّكون باعتماد تقنيات الآر إس إيه كمعايير معتمدة من الحكومة مستقبلاً، وبالتالي فقد ينتهي الأمر بمايكروسوفت إلىٰ أن تنحصر ملكيتها من هذه التقنية بمجموعة يتيمة من الخوارزميات. فهرع بيدزوس عائداً إلىٰ ردموند، ليقدم محاضرة وعرضاً للبرهان بشكل قاطع، على متانة واتساع ما لديه من حقوق الملكية الفكرية.

ولقد جاءت محاولة وكالة الأَمن القومي الأخيرة لتخريب الصفقة، حسب الرواية التي رواها بيدزوس، حينما اتصل أحد مسؤولي الوكالة بمرفولد، وقال له، ما فحواه، «دعكم من الخوارزمية «رسا». (يقول مرفولد أنه لا يذكر هذه الكلمات حرفياً، ولكنه يؤكّد أن وكالة الأَمن القومي أعربت لمايكروسوفت عن اعتقادها أن من الخطأ استخدام رسا: إنه خطأ كبير ترتكبه شركة البرمجيات العملاقة بارتباطها بشركة لا يُعتد بها).

وهنا ثارت ثائرة بيدزوس. فاتصل كما يذكر الآن بأعلى من عرفهم رتبة وراء السياج الثلاثي، وشرح له ما بلغه. وقبل أن يتمكّن هذا المسؤول من النطق بكلمة واحدة طلب منه تقييم الأمر والاتِّصال بمايكروسوفت والاعتراف لها بأن الوكالة ارتكبت خطأً فادحاً [حين قامت بالتشويش على الخوارزمية]. وقال له: «إذا لم يصوب هذا الأمر فلسوف يكون لعضو الكونجرس عن منطقتي شأن معك. وإذا لم يجدِ هذا أيضاً فلسوف يكون حسابك مع المدعي العام في المنطقة، لأني سوف أتقدم بالادعاء عليكم. وإن لم يجد هذا كذلك، فإني سوف اتصل بصحيفة نيويورك تايمز. ومهما يكن فإنكم إن لم تصلحوا الأمر، وجدتموني لا أدعُ سبيلاً حتى تتحمّلوا مسؤولياتكم». ولقد توقع بيدزوس أن ينكر محدّثه ما نسب إِلىٰ عناصر وكالته، إن كلياً أَو جزئياً، أَو يصر على جهله بأمر التخريب. ولكنه، بدلاً من ذلك، قال على ما يزعم بيدزوس: «لسوف اتصل بهم». ولقد اتصل محدثه حسب رواية بيدزوس، بمايكروسوفت معتذراً عما سلف من موظفي الوكالة [بحق الخوارزمية والشركة].

أصبح الطريق سالكاً الآن لعقد الصفقة. ولكن نقطة واحدة صغيرة وقفت تعرقل الاتفاق هي إصرار بيدزوس على أن يوقع بيل جيتس العقد شخصياً، ولقد كان بيدزوس يريد عرض الصفحة الأخيرة من العقد على حائط [مكتبه]، وكيف يبدو الأمر بدون جون هانكوك مدير عام مايكروسوفت الشهير؟ ويقول

مرفولد متفاخراً أنّه استطاع بتلميحه إلىٰ احتمال تعذّر توقيع العقد من بيل جيتس شخصياً أن ينتزع من بيدزوس بعض السكاكر. (ولكن بيدزوس أيضاً نال قطعة سكر بدوره، حضور جيتس حفلاً في الآر إس إيه).

وبعد بضعة أيام، وفي عطلة نهاية الأسبوع، في ذكرى قتلى الحرب [يصادف يوم الاثنين الأخير من شهر أيار/ مايو] 1991، اتصل بيدزوس بفوجنر، وهو يتباهى بالصفقة التي بلغت اكتمالها الآن. ويذكر فوجنر أنه عجب لذلك، وقال لبيدزوس: «هذا عجيب، يا جيم. لديك مايكروسوفت، لتشتري رخصة عدة شركتك الخاصة، ثم ها أنت ذا تضمنها نظام التشغيل لديهم؟ هذا لا يصدّق! كيف استطعت ذلك؟».

فقال جيم بيدزوس: «هكذا فن الإقناع والبيع، يا بوب، وأنا بائع ممتاز!».

وسواء كان الأمر يتصل بفن الإقناع والبيع أم لا، فقد بات مستقبل المفتاح العام، في أوائل 1991، موضوع شك، بسبب افتقاد موافقة الحكومة. كان بيدزوس يتحرّق طبعاً لتكون الخوارزمية رسا المعيار للشيفرة. والحق أن المؤسّسة القومية للمعايير والتكنولوجيا شديدة الحماس في بداية العملية لإرساء رسا معياراً. فقد كتب عالم كبير في المؤسّسة يصف «رسا» بـ «نظام مفتاح عام شامل رفيع جداً». بل لقد حاولت المؤسّسة حتى في كانون الأول / ديسمبر 1990 أن تقنع خصم بيدزوس، وكالة الأمن القومي ـ التي كان صوتها في العمليّة حاسماً ـ بضرورة اعتماد هذا النّظام، إذ قال مندوبوها في اجتماعات وكالة المخابرات أن من مزايا النّظام رخص كلفته تجارياً، كما أنّه ليس هناك ما يضارعه من الناحية الفنية.

ولكن المفاوضات تعرقلت بعد هذا، كما لم تُجدِ المناشدة كما يبدو من بيدزوس أَو فوجنر في اعتماد رسا معياراً. ثم بدا السبب في ذلك جلياً يوم 30

آب/ أغسطس 1991. ففي هذا اليوم توصَّلت وكالة الأَمن القومي إِلىٰ طريقتها الخاصَّة في التشفير.

ولقد طرحت المؤسَّسة القومية للمعايير والتكنولوجيا مجموعة جديدة من الخوارزميات، عبر المدونة الفيدرالية The Federal Register، لتكون المرشح الأول بين المعايير. وكان هذا المنتج الحكومي المعروف باسم «خوارزمية التوقيع الرقمي» DSA، قد وضعه موظف في وكالة الأَمن القومي يدعى ديڤيد كرافيتز، وهو مشابه في الكثير من النواحي لمخطط توقيع «رسا». وكلاهما يستخدم زوجاً من المفاتيح العامة ـ الخاصة. وفي كلاهما على أليس، حين تشاء كتابة رسالة موقّعة رقمياً، أن تنفذ خوارزمية تُعرف باسم دالة التجميع وتؤدي إِلىٰ «مختصر الرسالة». (وهذا اختصار للرسالة والإبقاء على جوهرها لتيسير المعالجة). ثم يكون تشفير الرسالة، أَو «توقيعها» عبر عمليَّة رياضية تعتمد على المفتاح الخاص الفريد الذي تحمله أليس، وترسل كلتا الرسالتين الأصلية والمختصرة إِلىٰ بوب على الطرف الآخر. وحين يستلم بوب ـ أَو أي شخص آخر ـ الرسالة يكون لديه الآن طريقة للتحقّق من أن صاحبتها هي أليس فعلاً ولم تتعرّض لعبث من عابث أَو أي شيء من هذا القبيل، أثناء البث: وهي أن يستخدم عندئذ مفتاح أليس العام لعرض الرسالة والملخص. ثم يتوسل بدالة التجميع ليعيد تكوين رسالة أليس من الملخص. فلا تتطابق الرسالة المكوّنة والأصل، إِلاَّ إذا كانت قد صدرت الرسالة عن أليس وإِلاَّ ظلَّت الرسالة على حالها دون تبديل.

كانت طريقة الحكومة تختلف عن مخطط التوقيع بطريقة «رسا» من ناحية واحدة، وهي أَنَّه لا يمكن استخدام المفتاح العام ـ الخاص المزدوج إِلاَّ للتثبت من هوية المرسل، وليس للتشفير؛ أي بعبارة أخرى أن هذا نظام مفتاح عام لا يقوى على حفظ سر، وهكذا فإنَّه لا يمثِّل خطراً على الأمن القومي، أَو حفظ النِّظام، أي أنَّه بدقيق العبارة عين ما أرادت الحكومة. وقد قال مسؤول في

المؤسَّسة القومية للمعايير والتكنولوجيا، في شهادة أمام الكونغرس: «إن استراتيجيتنا الأساسية تهدف إلىٰ تطوير تكنولوجيا تشفير لا تلحق ضرراً بأمننا القومي ولا تنال من قدراتنا على حفظ النِّظام في هذا البلد. . . ولقد كان هدفنا ابتكار تكنولوجيا تنفيذ تواقيع ـ ولا شيء آخر ـ بشكل متقن».

ولكن المؤسَّسة القومية للمعايير والتكنولوجيا لم تأخذ بهذا الهدف، وهي التي كانت تحبِّذ أصلاً اعتماد الحل الذي أتت به الآر إس إيه، إلاَّ إثر ضغط مارسته عليها فورت ميد [وكالة الأَمن القومي]. ففي الشهور الأخيرة من 1990، كانت وكالة الأَمن القومي تتشدد في الدعوة إلىٰ اعتماد نظامها، ثم طرح الموضوع مديرها الجديد الفريق وليم ستيودمان، في شباط/ فبراير 1991، وألحَّ على المؤسَّسة القومية للمعايير والتكنولوجيا بأن «تختصر النقاش وتقوم بإجراء ما يلزم لتوفير الحماية الضرورية».

وفي الاجتماع التالي لمجموعة العمل المشتركة التي تضم أعضاء من الوكالة والمؤسَّسة رفع ممثلو المؤسَّسة الأعلام البيضاء، إعلاناً بأن إداراتهم، «تقبل اقتراح وكالة الأَمن القومي». ولكن حين أعلنت المؤسَّسة القومية للمعايير والتكنولوجيا اعتماد خوارزمية وكالة الأَمن القومي في نيسان/ أبريل لم يأت أحد بأي إشارة إلىٰ علاقة وكالة المخابرات السرِّيَّة بالأمر.

غير أن بيدزوس لم يخدع بظواهر الأمور، وثارت ثائرته لاختيار الحكومة خوارزمية التوقيع الرقمي معياراً. ثم ذهب إلىٰ القول بأن وكالة الأَمن القومي قد تمكَّنت من تخريب وزارة التجارة ـ وهي تخضع لها المؤسَّسة القومية للمعايير والتكنولوجيا ـ تخريباً كاملاً. ومضى في ادعائه، بأن وزارة التجارة أصبحت تعمل ضد الصناعة الأمريكية، عوضاً من دعمها، وغدت في خدمة الأشباح كلياً. (ولقد دعم هذا الشك في ما بعد تحقيق قام به الكونغرس وحمل لجنة مراقبة العمليات الحكومية على الإعلان بأن «NSA وكالة الأَمن القومي» لا تصلح للقيام بهذا المشروع الهام»). وحذَّر بيدزوس من أن الخطوة التالية

ستكون افتضاح معيار للتشفير لا يأخذ بالخوارزميات المعروفة ـ خوارزمياته! ـ وإنما خوارزميات جديدة تستطيع الحكومة تفكيكها.

لقد كان في جعبة بيدزوس الكثير من القنابل ليستخدمها في هجومه. فمن ناحية فنية محضة، كان واضحاً أن خوارزمية «التوقيع الرقمي» DSA دون خوارزمية «رسا» متانة، فكانت «معياراً غريب الأطوار»، على حد تعبير أحد المراقبين، وأبطأ من خوارزمية رسا في التحقّق من التواقيع (وإن كانت أسرع منها في توقيع الرسائل)، وأشد صعوبة في التطبيق وأكثر تعقيداً من الأخرى. ولم تكن تتضمَّن عنصر التشفير، ولا كانت تتمتّع بسجل وصف مسار، على العكس من «الرسا». ومع ذلك فقد كان المبتكر الحكومي يتمتع بميزة على «الرسا»، وكان على بيدزوس أن يسعى جاهداً ليأتي بمعادل لها. فقد أعلنت الحكومة، في البيان الصادر يوم 30 آب/ أغسطس، اعتزامها توزيع معيار التوقيع الذي خرجت به على نطاق عالمي مجاناً دون أجر.

ورأى بيدزوس أنه قادر على مجابهة المعيار المقترح متوسلاً في ذلك بحقوق الملكيَّة الفكريَّة. ولكن الأمر لن يكون يسيراً. فقد كانت الشركة ببليك كي بارتنرز PKP تسيطر على حقوق الملكيَّة الفكريَّة للمبتكرات الخاصة بجامعة ستانفورد التي تتضمن أول التواقيع الرقمية. ولكن الحكومة ادعت بأن مخطّطها قد تجاوز تلك البراءات وذلك بالاعتماد على تطبيق مغاير من التواقيع الرقمية. وكان هذا المخطط قد صُمِّم على يد كريبتوجرافي من ستانفورد يدعى طاهر الجمل، وهو من طلاّب هيلمان القدامى، وقام بوضع وصقل فكرة الخوارزمية المجمعة وتلخيص الرسالة من أجل التوقيع الرقمي. غير أن الجمل أخطأ بأن قام بنشر مشروعه قبل التقدم بطلب براءة الملكيَّة الفكريَّة (صدر بحثه عام 1985)، فكان أن تخلّى بذلك عن حقوق براءة الاختراع. فإذا كان زعم الحكومة صحيحاً فإن خوارزمية المفتاح الرقمي تصبح متاحة مجاناً ولا يترتب على استخدامها أي حق بادعاء الملكيَّة الفكريَّة.

ولكن بيدزوس ذهب مذهباً مخالفاً، إلاَّ أنَّه أدرك أن عرض القضية للتحكيم هدر للوقت ومكلف مادياً. ومع ذلك فقد وجد طريقاً آخر لاتهام الحكومة بسرقة الملكية الفكرية. وكان هذا يتطلب براءة أخرى.

كانت هذه البراءة تقوم على عمل لعالم شيفرة ألماني، يدعى كلاوس شنور، حصل على براءة الملكيَّة الفكريَّة عن مخططه للتوقيع الرقمي في شباط/ فبراير 1991. وقد أصرّ شنور بعد سماعه بخوارزمية التوقيع الرقمي على أن هذه الخوارزمية تنال من حقوق ملكيته الفكرية وطالب الحكومة الأمريكية بمليوني دولار تعويضاً عن الضرر الذي لحق به. وكان هذا الادعاء في رأي العديد من المراقبين مبالغاً فيه من طرف شنور لأن كلا النظامين، سواء كان هذا الذي أتى به شنور أم ذاك الذي ابتكره كرافيتز، هما نسختان عن نظام طاهر الجمل. ومع ذلك فقد أثار الأمر قلق الحكومة. ذلك أنَّها تجشمت عناء كبيراً، بتأكيدها عند طلب براءة الملكيَّة الفكريَّة على أن الأفكار التي يقوم عليها خوارزمية التوقيع الرقمي لم تُستق من شنور. غير أن شنور كان لديه بعد براءة «فزاعة» واحدة على الأقل: ادعاء قد يمكن أن يصمد في دعوى طويلة محكمة، إلاَّ أنها توفر للمدعي سبباً وجيهاً لمهاجمة مفهوم مماثل. وإذا لم تتم تسوية الأمر مع شنور، فإن الحكومة ستواجه مشكلة.

ولقد رأى بيدزوس في هذا الوضع، فرصة عظيمة يمكنه اغتنامها. كانت الحكومة ترتعد أمام المشكلة الناشئة، شرع وهو يحاول إضافة البراءة الألمانية إلى مجموعة البراءات لدى ببليك كي بارتنرز، أي بعبارة أخرى تأسيس احتكار لبراءات الملكيَّة الفكريَّة! وصادف أن علم بيدزوس أن شنور كان يشارك يومئذ في مؤتمر علمي في مارسيليا. وهكذا طار وفوجنر للقائه. ووُفِّقَ الاثنان في الاجتماع به على غداء، في أحد أفخم المطاعم في المدينة. ولقد طال الغداء وامتد عدة ساعات. وكان شنور في الأربعينات، وعالماً محافظاً، ويزهو بأحدث فتوحاته العلمية، إذ كان قد نال جائزة لايبزيج لتوه ومكافأة مالية

مجزية. وتفتق ذهن بيدزوس بسرعة عن طريقة للتعامل معه: «لقد تحدثت إليه كما يتحدَّث مدرب مع لاعب التينس، وقلت له أنه يستطيع تنفيذ الخوارزمية بنفسه، أَو يدع لي التفاوض وتولي الاهتمام بعقوده والتراخيص، ويستطيع عندئذ التفرغ لاهتماماته العلمية». وقد أثارت هذه المفاوضات إعجاب فوجنر: «لقد أغرقه بقصص عن صداقته مع بيل جيتس وتصوره لمفتاح عام للشيفرة يعم العالم والكون».

وانتهت الوليمة في خاتمة المطاف، بينما الندلاء يقفون، يستعجلون تنظيف آخر الموائد. ثم انتقل الثلاثة إِلىٰ حانة في منطقة الميناء. وهناك قام فوجنر بتدوين اتفاقية على ورقة تنتقل بموجبها كافة الحقوق الناجمة عن الملكيَّة الفكريَّة التي تخص شنور إِلىٰ ببليك كي بارتنرز PKP. في تلك الحانة، وفي ظل سفينة شراعية من القرن الخامس عشر وقَّع شنور الورقة، سواء تحت تأثير وعود بيدزوس بالثراء أم بسبب التعب الذي نال منه.

ولما عاد بيدزوس إِلىٰ الولايات المتّحدة كان له لقاء آخر من سلسلة لقاءات لا تنتهي، مع المؤسَّسة القومية للمعايير والتكنولوجيا. وكان اتِّصاله محدداً بدينيس براندستاند ولين ماكنلتي، وهما عالمان من علماء الكومبيوتر في الوكالة، غالباً ما وجدا نفسيهما بين مطرقة مطالب الجمهور وسندان أوامر رؤسائهما. وقد بذل هذان العالمان أقصى جهودهما لحثّ المؤسَّسة القومية للمعايير والتكنولوجيا على شراء حقوق الملكيَّة الفكريَّة لمبتكر شنور، أملاً منهما بحل مشكلة البراءة الفكرية التي تواجه الحكومة. كذلك سعى العالمان إِلىٰ تسوية أي نزاع حول الملكيَّة الفكريَّة التي تعود لجامعة ستانفورد بدفع تعويض مالي إِلىٰ شركة الآر إس إيه. وعليه فقد ذهب بهما الظن إِلىٰ أن الاجتماع سوف ينحصر بالتداول في مثل هذه المسائل. ولما بدأ الاجتماع وجدا بيدزوس يبادرهما بالقول: «إني أمثّل كلاوس شنور وأنتم معتدون على حقوقي بالملكيَّة الفكريَّة».

ولقد غمر بيدزوس شعور عارم بالنشوة في هذا اللقاء، حتى أنه استذكره في ما بعد، وقال: «إنني لم أر في حياتي شخصين بلغ بهما التعب هذا المبلغ».

وراح بيدزوس، في غضون ذلك، ينظم حملة معارضة لخوارزمية التوقيع الرقمي على جبهات أخرى. فقد تلقت المؤسَّسة القومية للمعايير والتكنولوجيا، رداً على الإعلان في المدونة الفيدرالية يوم 30 آب/ أغسطس، تعليقات على الخطة، ومعظمها كانت انتقادات. وكانت الشركات التي تستخدم الخوارزمية «رسا»، ومنها مايكروسوفت ولوتس، قد أزعجها أن تجد استثماراتها في هذه الخطة تذهب هباء، وأن تضطر لتطوير برمجيات جديدة للمعيار الجديد. وكان ثمة انتقادات أخرى موجّهة لبطء معدل سرعة عملياتها الحسابية. كذلك اهتم النقّاد بضعف مخطط خوارزمية التوقيع الرقمي. لأن المعيار المقترح لا يستخدم سوى المفاتيح من 512 بت لحساب التواقيع (تستخدم رسا 1024 بت) كان ثمة شك بقدر الكومبيوتر الضخمة في السياج الثلاثي على أن تطرح توقيعات مزورة. وكيف يمكن لكائن من كان أن يؤكد أن توقيعاً ما صحيحاً في حين أن لدى وكالة للاستخبارات الإمكانات للقيام بأعمال التزوير؟ وكان الأمر كله عند رون رايفست رمزاً لسياسة الحكومة عموماً. لذلك طرح سؤاله في مؤتمر عقد في واشنطن العاصمة في عام 1992: «أية سياسة للشيفرة ينبغي على هذا البلد أن يأخذ بها؟ هل يأخذ برموز قابلة للتفكيك أم شيفرة عصية على الحل؟».

ومع أن الجدل لم يتطور إلىٰ نقاش واسع بين الجمهور عامة، إلاّ أنه أثار مع ذلك حماس بعض جماعات الدفاع عن الحريات المدنية التي كانت تراقب عن كثب العلاقة بين وكالة الأَمن القومي، والمؤسَّسة القومية للمعايير والتكنولوجيا. والحق أن ميزان القوى بين الهيئتين، كان مدعاة للسخرية، فهذه سفينة القيادة لعملياتنا الاستخباراتية بميزانية عدة بلايين من الدولارات والأخرى

مخزن متواضع من مخازن الحكومة. ولئن كان الليبراليّون، والمتحرّرون يأملون من هذه المنظمة الأخيرة، أن تقوم بحماية مصالح المواطنين العاديين، فإن ثقتهم بأن تتمكّن المؤسّسة من تحقيق هذا الأمل كانت ضعيفة.

وكان للمخاوف التي تراود هؤلاء ما يبرّرها. فإن ألقى المرء نظرة على تاريخ هاتين المنظمتين، وجد أمامه صورة لاختلال موازين القوى. فبعد جلسات لجنة السيناتور تشيرش في السبعينات شعرت وكالة الأَمن القومي أن تنظيمها كله لم تبرأ ساحته بل عوقب. ولكن الحكومة أخذت تبدي في عام 1984، في ذروة سلطة رونالد ريغان في الرئاسة، ما ينم عن عودتها إِلىٰ عالم السياسة الداخلية. فبناء على طلب واضح من فورت ميد، أصدر الرئيس ريغان توجيهاً يتصل بالأمن القومي برصد قواعد البيانات المعلوماتية داخل الحكومة وخارجها والتي تقع في حيز المعلومات «الحسّاسة» ولكن غير السرِّيَّة، سواء كان مصدرها الحكومة أم غيرها. وقد أدّى هذا إِلىٰ إثارة استياء شديد. وفي النهاية قام النائب عن تكساس جاك بروكس، خصم وكالة الأَمن القومي في الكونغرس، بتوجيه أقسى النقد إِلىٰ الوكالة؛ فقال في إحدى جلسات الاستماع: «إن قبو البيت الأبيض والغرف الخلفية في البنتاغون ليسوا بالأَماكن التي ينبغي أن تُرسم فيها سياسة للبلاد». وكان أن تراجعت الحكومة وانسحبت من الساحة.

ولقد حملت هذه التجربة بعض أعضاء الكونغرس، مدفوعين بضغط من جماعات حماية الحريات المدنية، على وضع قانون يرسم الحدود للحكومة في عصر الكومبيوتر. فأصدر الكونغرس في ما كان تصرفاً غير مألوف يعبر عن استقلاله عن مطالب وكالة استخبارية، قانون أمن الكومبيوتر لعام 1987 الذي أحال مسؤولية حماية أمن البنية التحتية للكومبيوتر، وخاصة بما يتصل بتزكية المعايير التي ينبغي على هذه الصناعة أن تلتزم بها، من وكالة الأَمن القومي إِلىٰ المكتب القومي للمعايير حصراً (وكان على وشك أن يتخذ الاسم الذي يدل على ارتفاع المكانة، وهو المؤسّسة القومية للمعايير والتكنولوجيا).

والسؤال هو، إذن، لماذا كان تنديد الكونغرس بأشباح وكالة الأَمن القومي؟ حقاً أن جماعات الدفاع عن الحريات المدنية قد مارست ضغوطاً شديدة على دوائر الكونغرس. ولكن الأهم، على حدّ قول مارك روتنبيرج، وكان يومئذ مستشاراً للسيناتور باتريك ليهي، «إن الفعالية التجارية الأمريكية لم تكن لترتاح، إلىٰ تولي وكالة الأَمن القومي وضع المعايير. فالمخاوف التي تراود وكالة الأَمن القومي بشأن أمن الكومبيوتر ليست المخاوف ذاتها التي تواجه التجارة ـ فالفعاليات التجارية لم تكن لتقلق بشأن الكرملين، وإنما ما كان يقلقها هم المنافسون».

ولما لمس المشرعون تأييد رجال الصناعة تحركوا بسرعة وباتت وكالة الأَمن القومي، عاجزة عن اللحاق بمجريات الوضع. بل ما كان حتى لظهور الفريق وليم أودم مدير الوكالة يومذاك أن يمنع صدور القانون. أما شكواه من أن إحالة مسؤوليات أمنية إلىٰ جهة مدنية «ازدواج» للوظائف لا ضرورة له فقد فاته فيها إدراك المقصود، وهو أن أصحاب الصناعة يؤثرون أن تتولّى وزارة التجارة، لا الجواسيس، وضع المعايير للبنية التحتية للكومبيوتر التي تستخدمها القاعدة العريضة من الشعب. وكما ذكر أحد مسؤولي الوكالة لاحقاً في مذكرة له: «لقد استغرقنا وقتاً لاستيعاب المقصود. . . كان [النائب جاك بروكس] قد تمكّن من حشد التأييد بالإجماع، للقرار بالشهادة والتصويت».

لم تستبعد «القلعة»، من عملية ضبط أمر الأمن، للحواسب المصنعة في البلاد كلياً. ذلك أن الوكالة كانت تتمتع بخبرة لا تقدّر بثمن، في مجال الأمان، فهي عاصمة الكريبتو في العالم بلا منازع، ولذلك فإن الكونغرس رسم لفورت ميد دوراً بأن أناط بها مهمة القيام بدور استشاري إلىٰ جانب المؤسَّسة القومية للمعايير والتكنولوجيا. وكان السؤال كيف يمكن للمؤسَّسة والوكالة أن تعملا معاً؟ في المفاوضات التي جرت لتحديد أسلوب العمل اتّخذ مندوبو الوكالة مقاعدهم مقابل مدير المؤسَّسة المكلّف، وكان بيروقراطياً يدعى رايموند

كرامر. ولم يكن كرامر هذا عطوفاً على وكالة الأَمن القومي وحسب، بل كان في الواقع ابن اثنين من قدامى الموظفين فيها! حقاً إن مذكرة التفاهم، التي توصلت إليها المؤسَّسات قد حافظت على التصور بأن تقود المؤسَّسة عملية وضع المعايير، إلاَّ أنَّها صاغت للوكالة دوراً رسمياً في كافة القضايا التي تتصل بالخوارزميات وتقنيات الشّيفرة»، كما ورد في المذكرة، وعلى المؤسَّسة القومية للمعايير والتكنولوجيا أن تطلب معونة وكالة الأَمن القومي في هذه الأمور. ولتنفيذ هذا البند تعين على الهيئتين أن تتعاونا معاً عبر «مجموعة عمل فنية». ولئن كان يفترض بأن تتولّى المؤسَّسة مسؤولية العملية إِلاَّ أنَّها لم تكن تتمتّع بالأغلبية في المجموعة التي كانت تضم ثلاثة أعضاء من كل هيئة.

ومع أن كلاً من الهيئتين كانت تؤكّد أن القيادة هي حقاً للمؤسَّسة القومية، إِلاَّ أن أهل الريبة كانوا يشكّكون في هذا القول. وفجأة أصبحت المؤسَّسة القومية للمعايير والتكنولوجيا حتى مع اسمها الطنّان الجديد المتذمر الحصيف في الحكومة، وسط معركة سياسية وأمنية قومية ضخمة. وقد اعترف واحد على الأقل من كبار المسؤولين في وكالة الأَمن القومي، في ما بعد بأن المؤسَّسة القومية للمعايير والتكنولوجيا لم تسع إِلىٰ امتلاك السلطات التي منحها إياها قانون الأمن ولا رغبت فيها بعد إقرار القانون، وعلى حد قول هذا المسؤول لقد وضعتنا في موضع المسؤولية عما لم نكن نرغب في تحمّل مسؤوليته».

ولقد بدت المناوشات حول معيار التوقيع الرقمي، أكبر برهان على تبعية المؤسَّسة القومية لـ فورت ميد [وكالة الأَمن القومي]. وقد جاءت التحقيقات في السنوات اللاحقة شاهداً على ذلك؛ وهناك تقرير من مكتب الحسابات العامة نطالع فيه خلاصة [تجربته] التي جاء فيها أن المؤسَّسة على العكس من القصد الذي شاءه الكونغرس «تتبع أثر وكالة الأَمن القومي في تطوير معايير تشفيرية معينة». وتوضح الوثائق التي كُشف النقاب عنها وتعرض للمناقشات

التي كانت تدور في الاجتماعات الشهرية لمجموعة العمل الفنِّيَّة هذا بجلاء. وتظهر أن جماعة المؤسَّسة القومية كانت تنتظر حكم وكالة الأَمن القومي في كل خطوة تتعلَّق بموضوع التوقيع.

بل لقد عانت مجموعة الرقابة التابعة للمؤسَّسة القومية للمعايير والتكنولوجيا ذاتها، وهي مجلس سلامة وأمن نظام الكومبيوتر، من مشكلات حادة كانت تعترض العلاقة بين الهيئتين. ففي آذار/ مارس 1992 رأى هذا المجلس أن مراجعة علنية على المستوى القومي للآثار الإيجابية والسلبيَّة لانتشار استخدام المفتاح العام والخاص في التشفير باتت ضرورية». غير أن وكالة الأَمن القومي التي لم تكن ترغب في مناقشة أَو عرض الموضوع تمكّنت من القضاء على هذه الفكرة. وقد عبَّر مدير وكالة الأَمن القومي المعيَّن حديثاً، الأدميرال مايك مك كونيل في مذكرة سرِّيَّة، عن هذا الوضع بصراحة لا لبس فيها، إذ قال: «إن لدى وكالة الأَمن القومي تحفظات فيما يتصل بإجراء نقاش علني حول الكريبتوجرافيا».

ومع ذلك فقد بدأت الحكومة تستشعر بعض الضغط. وعاد النائب جاك بروكس إِلىٰ عقد جلسات الاستماع من جديد. فقدم فيها منتقدو وكالة الأَمن القومي شهادات محرجة. فقد أدلى ناتان مرفولد من مايكروسوفت بشهادة ذكر فيها إن نشر الحكومة معيارها للتوقيع المقترح، بما حفل من عيوب فنِّيَّة. . . جعل من المستحيل على صناعة الكومبيوتر، أن تعتمد المعيار الذي وضعته الحكومة في أغراض التجارة». أما أديسون فيشر، وهو من أوائل المستثمرين في شركة آر إس إيه داتا سيكيوريتي، وقد سبق له أن استخدم خوارزميات الشركة في منتجات الكومبيوتر الضخم في شركته الأم أورد في شهادته تعبيراً قوياً قدر له أن يتردّد في المناقشات التالية؛ إذ قال: «إن الكريبتوجرافيا وخاصة ما يتصل منها بالمفتاح العام باتت الآن في صميم التيار. إنها ببساطة جني آخر

من سلالة جن التكنولوجيا، وهو شديد النفع ولا يمكن إعادته إِلىٰ المصباح، وإن كانت له بعض الآثار الجانبية المنفّرة».

لقد كان لكل هذا النقد، وقع الموسيقى على أذني جيم بيدزوس. ومع أنّه غدا فارساً مدافعاً عن حرية التشفير، فقد كان هدفه الرئيس على الدوام تدعيم شركته. وكان مذهبه أن عملية المعايير، ربما سارت في النهاية حسب هواه، إذا استمر الضغط على الحكومة وتابع التهديد، باستخدام براءة اختراع شنور في المعركة، ضد مرشح الحكومة، فتفوز تقنيات الخوارزمية رسا بالموافقة، على اعتبارها معيار التوقيع الرقمي رسمياً.

ثم، تراجعت الحكومة. أَو هذا ما بدا على الأقل.

وحسب رواية جيم بيدزوس، كانت الحكومة قد توصلت في النهاية إِلىٰ نتيجة مفادها أن المعيار الذي أخذت به سوف يسقط ليس لاعتبارات تتصل بالشّيفرة وإنما لأسباب تتعلّق ببراءة الملكيَّة الفكريَّة. وفي اجتماع عُقد في حزيران/ يونيو 1993 في وزارة التجارة، سمع بيدزوس محام يمثّل المؤسَّسة القومية للمعايير يقول ما كان يتوق دوماً لسماعه: «إننا نود التعاون وإياكم». وتابع المحامي كلامه وبيدزوس ومحاموه يصغون مذهولين: «لم لا تقدمون لنا عرضاً لاستغلال الترخيص إذا شئتم تعويضاً؟»

فقال بيدزوس أنه سوف يبلغهم رده خطياً. وبدأت المفاوضات، مع تقديم الحكومة عرضاً مالياً سخياً للتعويض لبليك كي بارتنرز: احتكار الحكومة لبراءة التوقيع الرقمي، أي حق استخدام حكومة الولايات المتّحدة لخوارزمية التوقيع الرقمي معياراً مقابل منح الشركة ببليك كي بارتنرز نسبة من العائدات. وقدرت هذه النسبة بدولار واحد عن كل مستخدم. ولما كان هذا الاتفاق يعد بملايين الدولارات من العائدات، إذ يتحتم على كل مواطن أن يستخدم هذا المعيار في مراسلاته مع الحكومة في كل أمر بدءاً من إبرام العقود إِلىٰ الإفادات الخاصة بالضرائب، فإن ثمة حافزاً كبيراً يحمل بيدزوس على قبول

العرض. وهذا ما كان. وكان يتصرف بهذا المعنى على أساس الحد الأدنى الذي تقبل به الشركة، وضد مصالح الجمهور الواسع من الناس. فشركته سوف تصبح في النهاية، شريكاً في استخدام منتج لوكالة الأَمن القومي كمعيار، خوارزمية عرَّض بها بيدزوس ذاته علانية.

أخذ البعض يتساءل يومذاك، إن لم تكن استراتيجية الآر إس إيه في حماية الشّيفرة ببراءات الملكيَّة الفكريَّة ذاتها طريقاً إِلىٰ عرقلة تقدم الحرية الشخصية في استخدام الكومبيوتر. ولربما كان بيدزوس ذاته متحالفاً مع أشباح الظلام، جواسيس وكالة الأَمن القومي. ففي النهاية، «كان أحد الأهداف في نظام براءات الملكيَّة الفكريَّة التشجيع على استثمار التكنولوجيا. . . ولقد مضى على ابتكار كريبتوجرافيا المفتاح العام عشرون عاماً، ومع ذلك لم يقدّر له أن ينتشر. ولو قام المرء بزيارة مخزن كبير، سوبر ماركيت، ووقف عند الصندوق لما وجد توقيعات رقمية. فلماذا؟»، كما لاحظ أحدهم.

لكن الصفقة لم يقدّر لها أن تنتهي. ذلك أن الحكومة في استعجالها الانتهاء من معركة براءة الملكيَّة الفكريَّة لم تقدر الثورة التي ستنجم، عن نكوصها عن التزام سبق أن قطعته بتوزيع الخوارزمية مجاناً. ولما طلبت التعليق على الصفقة كان النقد الذي صدر شديداً، حتى أن النقَّاد وصفوها بهبة من بليوني دولار تقدم لببليك كي بارتنرز. كذلك ألمحت الحكومة الكندية، والمفوضية الأوروبية بأنهما ستمتنعان عن دفع العوائد، ولتذهب براءات الملكيَّة الفكريَّة التي تدعي الحكومة الأمريكية ملكيتها إِلىٰ الجحيم. فكان هذا تمرداً لم تكن حكومة الولايات المتّحدة بحاجة إِلىٰ مواجهته. وهكذا كان أن تراجعت المؤسَّسة القومية للمعايير والتكنولوجيا عن العرض الذي قدمته لبيدزوس وأعادت تأكيدها أن المعيار الذي سوف تعتمده سيكون دونما عائدات. وهكذا عادت الأمور إِلىٰ نقطة البدء في موضوع معيار التوقيع الرقمي.

ولقد قابل بيدزوس هذا التحول بروح فلسفية، ولم يأسف لخسارة كل

تلك الأرباح، الضخمة المتوقعة بفضل هذه الصفقة. لكن الخطة فشلت. وما كان كان، وأصبح بوسعه أن يعود مرة أخرى إِلىٰ صف الملائكة، خصماً لحكومة تسعى، إِلىٰ القضاء على حرية الفرد الشخصية، ولو أدّى ذلك إِلىٰ إفقار شركات البرمجيات الأمريكية.

وكان مقدّراً للجدل بشأن معيار التوقيع، أن يستمر عاماً أخر. ولم تحسم المؤسَّسة القومية للمعايير أمرها، وتستقر على خيارها النهائي إِلاَّ في كانون أول/ أكتوبر 1994. فشاءت أن تصرف النظر عن موضوع براءة الملكيَّة الفكريَّة وتتجاهل ردّ الفعل السلبي الهائل من الجمهور الواسع وتزكية خوارزمية التوقيع الرقمي مرشحاً ليكون المعيار الرسمي للتواقيع الرقمية. فذكرت في نشرة حقائق المؤسَّسة أنها «راجعت كافة براءات الملكيَّة الفكريَّة وخلصت إِلىٰ أنَّه لن يكون هناك تجاوز على أي من الحقوق المترتبة على الملكية». (ولطمأنة أولئك الذين ما تزال تراودهم الشكوك، اتخذت المؤسَّسة خطوة استثنائية بتحمّل المسؤولية عن أي شخص يستخدم المعيار إذا ما تعرض لاحقاً للمقاضاة لانتهاكه قوانين الملكيَّة الفكريَّة). ومع أن المؤسَّسة القومية للمعايير قد أجرت بعض التعديلات الفنية المفيدة التي تختلف عن عرضها الأصلي، وأبرزها تمديد طول المفتاح من 512 بت إِلىٰ 1024 بت. فإن النتيجة كانت نظام تثبت، ابتكرته سراً وكالة الاستخبارات الحكومية، نظام لم يجد فيه أحد شيئاً من الجاذبية ليأخذ به بديلاً لنظام معتمد ومطبق من مايكروسوفت وأبل وآي بي إم ونوڤيل. فهل من عجب إذا ظل معيار التوقيع الرقمي يتيماً لا يوجد من يتبنّاه حتى بعد انقضاء الأعوام؟ وألا يوجد حتى في غمرة ازدهار صناعة الإِلكترونيات وسيلة عامة للتثبت في البريد الإِلكتروني؟

والمضحك في الأمر، كما قال العالم لين مك نلتي في المؤسَّسة القومية للمعايير والتكنولوجيا: «قد كنا نعتقد أن التوقيع الرقمي أمر يسير». لكن معركة التواقيع، على ما يبدو، رغم ما كانت عليه من الشدَّة، لم تكن سوى تمرين «إحماء» للحدث الرئيس في حرب الكريبتوجرافيا: حرب التشفير.

فوضى التشفير

عندما بدأ فيل زيمرمان مغامرته في الكريبتوجرافيا، لم تكن لديه أدنى فكرة بأنّه سيغدو بطلاً شعبياً، وفي الوقت نفسه سيخضع للتحقيق لانتهاكه القانون الفيدرالي. فقد قام بهذه المغامرة بدافع من فضوله العلمي، وولع الهاوي، وشيء من البارانويا السياسية. ولد زيمرمان عام 1954، وترعرع في عدد من مدن ولاية فلوريدا، ووصف نفسه «لست بطبعي شخصاً يهوى الحفلات». وكان شخصاً انعزالياً غريب الأطوار. ووالده سائق شاحنة؛ كذلك كان والداه يدمنان الكحول. أما هو فكان يطمح إِلىٰ أن يصبح عالم فلك. وعلى الرغم من أنَّه كان ما يزال في الصف الرابع الابتدائي، فقد استهوته الرموز حتى ملكت عليه عقله. وكان تلفزيون ميامي قد دأب على بثّ برنامج يدعى إم. تي. جريفيز وسجن المغارة، في فترة الظهيرة من كل يوم سبت، وكان يضم ناد للأطفال، ويباع لأعضاء النادي «مفتاح كالمفاتيح العادية لتفكيك رموز سرِّيِّة؛ وفي البرنامج كان يتم عرض عدد من الأَرقام تظهر على الشاشة بشكل ومضات، وعلى أعضاء النادي ترجمتها باستخدام المفتاح لتغدو رسائل سحرية واضحة. ولم يشتر زيمرمان المفتاح قط، إِلاَّ أنه، قام بتدوين الأَرقام على عجل واستطاع أن يحل الشّيفرة لتصبح نصاً بسيطاً واضحاً. فبالنسبة لطفل وحيد لعائلة مضطربة، كان تحويل هذه الرموز الغامضة إِلىٰ ما

هو مفهوم قد منحه إحساساً بالتفوّق، والانتماء. والإحساس ببيت منظم.

فلا عجب إذن إن يسعى الفتى لمعرفة المزيد عن الشّيفرة. وكان أن وقع على كتاب من تأليف هيربرت اس. زيم، وهو كاتب للأطفال، عنوانه «الرموز والكتابة السرِّيَّة»، من منشورات دار سكولاستيك. ليكون في متناول الأطفال بين سنّ العاشرة والاثنتي عشرة سنة. وهذا الكتيب نقل بطريقة مباشرة متعة الكريبتوجرافيا، وكأنما الكاتب موظف رفيع في المخابرات يقوم على تدريب مجنّد ذكي، إنما غرّ. وقد كتب زيم قائلاً: «ليس القصد من هذا الكتاب إعطاؤك رموزاً لتنسخها، بل مساعدتك على ابتكار رموز خاصة بك، لا رمزاً واحداً أَو رمزين، بل المئات منها، إن شئت، أما كيفية استخدام معرفتك بالرموز فأمر هو من شأنك».

لقد غدا هذا الكتاب، منذ ذلك اليوم، كتاب زيمرمان المقدس، وقام بحل كل ما فيه من التمارين، بكل أمانة وإخلاص، مثل صنع حبر سري من عصير الليمون، وابتكار شيفرات أصيلة، وبالطبع تفكيك الرسائل المشفرة في الكتاب. وبعد عامين، عندما كان في المرحلة الإعدادية، تباهى زميل له بشيفرة كان قد ابتكرها، وأن أحداً لن يستطيع حلّها، إِلاَّ أن زيمرمان قَبِل التحدي. وقال لزميله: «احرص على أن تجعلها رسالة طويلة». فاستجاب الفتى، معتقداً عن حمق أن رسالة طويلة ستكون أصعب حلاً. كانت الرسالة مكتوبة بأسلوب رموز الكتابة الرونية [أبجدية تيوتونية قديمة وعلامات تنطوي على معنى خفي أَو سحري. هـ. م]، وتذكر بشكل ضبابي باللغات التي تشيع في رواية توليكين: «مملكة الأرض الوسطى» [عمل شهير من أدب الخيال العلمي]. قام زيمرمان بتحليل الرسالة ونهج في ذلك منهج تحليل تكرار الرموز، وهو أسلوب بدائي في تحليل الشّيفرة يقتضي ببساطة حساب عدد المرّات التي تظهر فيها الأحرف الأبجدية. وذلك ما مكّنه من حلّها، وكأنَّها نص مشفّر عادي. فكان هذا الإنجاز مدعاة لدهشة صديقه كثيراً.

انحسر اهتمام زيمرمان بالشّيفرة، في سنوات المراهقة، ولم يدرك أن الكومبيوتر، يمكن أن تستخدم بوصفها أدوات تشفير حتى التحق بجامعة فلوريدا أتلانتيك. وعلى الرغم من أنّه كان متخصصاً بالفيزياء، إلاّ أن الأمر انتهى به أن أصبح يقضي معظم وقته في غرفة الكومبيوتر، ففي البدء قام بأعمال تتعلّق بتخصّصه، ولكن في النهاية راح ينهل من إكسير البرمجة ذاتها. وكان ما يجذبه إلىٰ ذلك ابتكار عالمه الخاص في الجهاز. إذ يقول: «يمكنك أن تتفاعل مع قطعة جماد، شيء بلا حياة، إلاّ أنه يبدو كذلك في ظاهره». وأجمل ما في ذلك أنه يجيده، بعكس كفاءته في الفيزياء. أما خصمه الرهيب فكان: حساب التفاضل والتكامل.

بالرغم من أنّه بدأ العمل بالترجمة منذ أسبوعه الأول في الجامعة عام 1972، إلاّ أنه لم ير كومبيوتراً حقيقياً طوال عام بأكمله، ذلك أن كليته كانت تمتلك محطات تتصل بآلات بعيدة فقط. فجامعة فلوريدا أتلانتيك ليست معهد ماساتشوسيتس للتكنولوجيا أَو جامعة ستانفورد. أَو حتى جامعة حكومية ضخمة. ثم أصبح زيمرمان طالباً مساعِداً، يعلّم الآخرين استخدام المحطات. وترك الفيزياء ليختص بعلوم الكومبيوتر.

وفي غرفة الكومبيوتر تلك، استعاد شغفه بالشّيفرة. وقد اقتضت إحدى تجاربه، كتابة رمز سرّي خاص به، مستخدماً لغة الفورتران المستخدمة في الكومبيوتر والتي باتت منسقة الآن. واستخدم في مشروعه مجموعة من الأَرقام العشوائية لاستبدال كل حرف في النص الواضح للرسالة بحرف آخر. وجعل عمل الأَرقام العشوائية يرتبط بمفتاح هو عبارة عن كلمة سرّيّة. ولما كانت رموزه لا يمكن حلها باستخدام التحليل الترددي (عمل العشوائية يقوم على تغيير حرف مثل التاء t الذي يظهر في بداية الرسالة إلىٰ حرف ما أما أحرف التاء اللاحقة فتستبدل بحروف أخرى). وظن زيمرمان أن وكالة المخابرات المركزية CIA ذاتها، عاجزة عن أن تحل هذه الرموز. فهو لم يكن ليتخيّل أبداً تقنيات

مثل الهجوم على نصّ واضح منتقى، أَو تفكيك مولدات الأرقام العشوائية. (ولم يسمع قط بوكالة الأَمن القومي). ولكن كان من المقدّر له أن يتصدّى لتلك الشّيفرة المنيعة ذاتها بعد سنوات حينما عرضت له في وظيفة مدرسية على أنّها شيفرة يمكن حلّها بسهولة باستخدام تقنيات أساسية في تحليل الشّيفرة. ويتحدَّث عن ذلك بقوله: «وهكذا كانت نهاية مخططي الباهر».

في صيف عام 1977، كان زيمرمان يعمل ـ في ذلك الحين ـ في شركة لصناعة أَجهزة الكومبيوتر الصغيرة في فورت لودرديل، ولم يكن قد بقي على تخرجه يومذاك سوى فصل دراسي واحد، وفي أثناء ذلك قرأ مقالاً نُشر في عمود ابتكارات رياضية في مجلة العلوم الأمريكية، وصادف أمراً أخذ بلبه. وكان ذلك بالطبع وصف مارتين جاردنر للمفتاح العام وخوارزمية رسا. ولما كان متعطشاً لمعرفة المزيد، اتصل برون رايفست في معهد ماساتشوسيتس، على نحو غير متوقع، وسأله عن إمكانية تطبيق النظام على الكومبيوتر. فأفاده رايفست بأن فريق معهد ماساتشوسيتس قام بذلك بأَجهزة ليست LISP [لغة برمجة لمعالجة القوائم. هـ. م.] أثناء اختبارهم للغة صوتية للكومبيوتر، تستخدم في الذكاء الصناعي. فقال له زيمرمان وقد شعر بخيبة الأمل: «إن ذلك يتجاوز طاقتي». إذ لم يكن لديه القدرة على الحصول على أَجهزة الـ ليسب المبهرة؛ فهي أدوات باهظة الثمن، تبلغ تكلفتها مئة ألف دولار، صممت لأغراض البحث، وليس لأداء مهمات عملية مثل الأعمال الحسابية. وعلى الرغم من أن زيمرمان لم يكن ضليعاً بعلم الحساب، إِلاَّ أنه أدرك أن احتمال حصوله على جهاز ليسب في جامعة فلوريدا أتلانتيك تكاد تكون معدومة. إِلاَّ أنه أخذ يفكّر في إمكانية تطبيق الخوارزمية رسا على تلك الكومبيوتر الصغيرة الحجم والرخيصة. فالأمر هنا مختلف. كان زيمرمان يمتلك حصة صغيرة من واحد من تلك الأَجهزة الصغيرة الرخصية الثمن المستخدمة حينذاك، والتي تصدر ضجيجاً وتعمل على معالج يدعى زيلوج زد ـ 80 Zylog Z-80 وهو نوع

من النموذج آ Model A كان مستخدماً في منتصف السبعينات. لكن بينما كان يفكِّر في أمر تطبيق خوارزمية رسا، أدرك أنَّه لا يعرف إلاَّ القليل عن كيفية القيام ببعض العمليات الحسابية المطولة المملّة التي تم شرحها في ورقة بحث فريق ماساتشوسيتس ولذلك تخلّى عن المحاولة.

في ذلك الوقت كان ثمة أمور أخرى، تجري في حياة زيمرمان. ففي السنة ذاتها التي اكتشف فيها الرسا، تزوج صديقته كيسي كافانو التي كانت عاملة مقسم في الكلية، وبعد فترة ليست بالطويلة، قام الزوجان بزيارة أصدقاء لهما في بولدر بولاية كولورادو، فأحبّا المنطقة كثيراً. ولما عاد زيمرمان إِلىٰ عمله في فلوريدا، راح يخطِّط للانتقال إِلىٰ تلك المنطقة. وبعد سنة حزم وكيسي أمتعتهما واستقلا سيارتهما الفوكسفاكن الصغيرة، وانطلقا إِلىٰ جبال روكي. وهناك حصل على عمل في شركة للبرمجيات لتصنيع محطة عمل معالج نصوص، وبدأ بتكوين عائلة: فقد ولد أول أبنائهما في عام 1980. ثم استمع إِلىٰ دانيل إِلسبورج وهو يتحدث إِلىٰ حشد في دينفر [ولاية أوهايو هـ. م] عن مناهضة التجارب النووية.

كان فيل زيمرمان، قد تجاهل في مرحلة دراسته الثانوية، حرب فيتنام إِلىٰ حد كبير. ولكن عندما درس في جامعة فلوريدا أتلانتيك أخذ يتبنَّى موقفاً سلبياً من الحكومة مناهض لها أشد ما تكون المناهضة. إذ أن فضائح نيكسون فتحت عينيه وكشفت له مبلغ الصفاقة التي يمكن للحكومة أن تبلغها في الكذب. ولما كانت رئاسة رونالد ريغان بلغ به الإستياء من السياسة حداً كبيراً. وكان قد قرأ كتاب روبرت شير With Enough Shovels، وانتابه قلق من احتمال إبادة البشرية بالقنبلة الذرية. فقرَّر زيمرمان وزوجه أن يرحلا إِلىٰ نيوزيلندا، إذ وجدا أنه من الحكمة أن يتجنّب المرء المحرقة المقبلة. وبلغ بهما الأمر حد الحصول على جوازات سفر وتجهيز أوراق الهجرة (لم يكن يعلم بعد أن صناعة الكومبيوتر في نيوزيلندا لم تكن ذات شأن). وفي عام 1982، حضر الاجتماع

الجماهيري الذي أُقيم في تلك السنة، واستمع إلىٰ إلسبورج، الذي أصبح من كبار الناشطين في مناهضة النشاطات النووية، بعد اللحظة المشهودة التي نشر فيها «وثائق البنتاغون». وهكذا انخرط زيمرمان في هذا التيار. ومنذ تلك اللحظة، نسي أمر الهجرة وقرَّر أن يصبح ناشطاً سياسياً، وأن يبقى ويقاتل.

كان زيمرمان وبعض أصدقائه، يقومون بتأسيس شيفرة، تدعى ميتا فوريك سيستمز، وقد عزموا على إنتاج لوحة مثبت عليها دارة كهربائية لأَجهزة أبل التي تعمل على تشغيل برامج متوافقة مع إينتل. لكن زيمرمان استطاع أن يجد الوقت ليبحث في كل كتاب يقع عليه في موضوعات سياسة الحلف الأطلسي، ومنظومات الأسلحة. . . إلخ وكان ينفق مئات الدولارات في مكتبة واحدة ويمضي الوقت بحثاً وتنقيباً في الكتب. وأخذ بعدئذ في تدريس السياسة العسكرية في الجامعة الحرة في بولدر. وتحدَّث في الاجتماعات الجماهيرية المناهضة للتجارب النووية وعمل مستشاراً لاثنين من المرشحين لعضوية الكونغرس، واعتُقل مرتين لمشاركته في تلك التجمعات. وفي إحدى المرات اعتُقل في المنطقة المخصّصة لإجراء التجارب الذرية في صحراء نيفادا، جنباً إلىٰ جنب مع بطليه إلسبورج وكارل ساجان. (إلاَّ أنه لم يوجه إليه اتهام في كلتا المناسبتين).

مع مضي عقد الثمانينات، بدا أن حركة مناهضة التجارب النووية أخذت تفقد زخمها. كذلك فإن شركة ميتافوريك سيستيمز لم تكن تبلي بلاء حسناً: فمنذ أن أصبحت لكومبيوتر آي بي إم الشخصية هي المسيطرة، باتت فكرة وضع معالجات إينتل، لكومبيوتر آبل ـ 2 ضرباً من السخف. وكان ذلك مدعاة لاضطراب زيمرمان نوعاً ما. إلاَّ أن كل شيء تغيّر بعد اتّصال هاتفي تلقاه من مبرمج يعمل في أركنساس، ولديه مشروع ما من أحد يقدره أكثر من فيل زيمرمان وقلّة قليلة من الناس.

كان هذا الشخص يدعى شارلي ميريت، واتضح أنَّه كان في الواقع يقوم

بالشيء الذي حلم به زيمرمان، منذ أن طالع مقال مارتين جاردنر في عام 1977: إذ كان يطبق الخوارزمية رسا في نظام المفتاح العام للتشفير على أجهزة كومبيوترات صغيرة الحجم. ذلك أن رد فعل ميريت كان يشبه رد فعل زيمرمان عندما قرأ عن الإنجاز الذي قام به الباحثون في معهد ماساتشوسيتس للتكنولوجيا (إم آي تي). وقد انتقل ميريت من مسقط رأسه في هيوستن (تكساس) إلىٰ فايتفيل في أركنساس، وهناك أسَّس وعدد من أصدقائه شركة، وبالفعل استطاعوا وضع برنامج مفتاح عام يعمل على كومبيوتر من نوع زد ـ 80. كان البرنامج يعمل ببطء شديد، إلاّ أن الابتكار نجح. لكن لم يكن هناك من يريد شراءه. وهكذا، بعد فترة من الزمن، انسحب أصدقاؤه جميعاً من الشركة، وبدأ ميريت وزوجته بتسويق البرنامج بأنفسهما. وفي النهاية وصلت أنباء مشروعهما التجاري الصغير إلىٰ العمليّة الاستخباراتية في فورت ميد التي أنفق عليها بلايين الدولارات. كانت وكالة الأَمن القومي ترسل مبعوثيها دورياً إلىٰ أركنساس لتحذير ميريت من العواقب الوخيمة التي قد تحدث إذا ما صدر برامج مشفَّرة خارج البلاد. ولما كان معظم زبائن برمجيات ميريت شركات تعمل وراء البحار وتنشد برامج تشفير تمنع عملاء الأنظمة الفاسدة المتنصتين، فإن هذا القيد جعل الشركة تغلق عملياً. وفي محاولة من ميريت، للحصول على بعض الحلول من داخل البلاد اضطر للاتّصال بشركات مغمورة كان قد قرأ عنها في المجلات المتخصّصة بأمل أن يرسلوا برامجه مع بضائعهم. وهكذا عثر على ميتا فوريك وفيل زيمرمان.

عندما سمع زيمرمان ما كان ميريت ينوي القيام به، شعر بسعادة غامرة حتّى حسب ميريت أن في الأمر خدعة: إذ لم يكن هناك أحد ممن قابلهم من قبل مفتوناً بالتشفير بمثل هذا القدر. وكان زيمرمان قد عبّر لميريت عن مقدار عشقه للتشفير، وعن أم تي جريفز وسجن المغارة، وهيربرت زيم ورون رايفست. كذلك عبّر له عن كرهه للأخ الكبير، [رمز السلطة الشمولية في رواية

جورج أورويل الشهيرة 1984 هـ. م]. لكنَّه أراد أولاً، أن يعلم كل شيء يعرفه ميريت حول جعل رسا تعمل على الكومبيوتر الشخصي.

والآن، بعد أن علم زيمرمان أن بالإمكان القيام بذلك، أصبح مدفوعاً لكتابة، برنامج المفتاح العام للتشفير الخاص به، للناس عموماً. ففي حين كانت جهوده السابقة في التشفير مجرد أعمال مأجورة، وتعبيراً عن شغفه بالرموز عموماً وحسب، إلاَّ أنَّه الآن أصبح ناشطاً سياسيّاً مثقفاً اعتُقل مرتين لتعبيره عن رأيه. كما يعلم أن الحكومة تمتلك في عصر الكومبيوتر أداة قوية لمراقبة المعارضة: ألا وهي الرقابة الإلكترونية. إذ لم يعد أمثال الأخ الكبير يقتصرون على التنصّت على المحادثات الهاتفية بآذانهم الكبيرة وحسب، ولكن بإمكانهم اقتلاع رسائل البريد الإلكتروني من الأثير الرقمي وقراءة المشاريع التجارية والأسرار المخزية إرضاء لقلوبهم السوداء القاتمة. ففي حين كان البريد الإلكتروني أمراً رائعاً، إلاَّ أنه في واقع الأمر مثَّل خطوة إلى الخلف فيما يتعلَّق بالخصوصية: فحتَّى بوجود البريد العادي غير الأمين نسبياً، كان الناس يقومون بإغلاق المغلفات لحماية سرية رسائلهم. والأمر الذي كان زيمرمان يأمله هو إنتاج المعادل الإلكتروني للمغلفات المغلقة. لكن إن أعطيت الناس برنامج تشفير لحماية البريد الإلكتروني، فسيكون لديك شيئاً أفضل من المغلفات المغلقة، وأعتقد، أنَّه في حال وافق الناس جميعاً على استخدامه، فسيكون ذلك نوعاً من التضامن، حركة جماهيرية لمقاومة التنصّت المقيت. فإلى الأمام، يا صاحبي!

ولما كان زيمرمان يعلم حدود سرعة المفتاح العام، فقد قدَّر أن برنامجه، يجب أن يكون نظام تشفير هجين. بحيث يستخدم نظام المفتاح العام «لرسا» البطيء لتبادل المفاتيح، وبعض الخوارزميات السريعة الأخرى، لتشفير كامل الرسالة. وكان لا يعلم ببرنامج لوتس نوتس، الذي كان يطبّق مثل هذا النظام الهجين، وبالتأكيد، يجهل تماماً شركة آر إس إيه داتا سيكيوريتي. والتي ستبني

تجارة كاملة، تعمل بوجب ترخيص مفتاح عام لتلك الأنواع من الأَنظمة التي اعتقد زيمرمان أنّه كان رائداً فيها. (كذلك لم يكن لديه أي فكرة عن براءات الملكيَّة الفكريَّة عن ابتكار رسا). وعلى أية حال، لم يكن لدى أي من الشركتين منتجاً للشحن في عام 1984.

أدرك زيمرمان عدداً من الأمور على الوجه الصحيح؛ منها أن البرنامج المفيد يجب ألا يقتصر في عمله على نوع واحد من الكومبيوتر، وإنما ينبغي أن يكون متوافقاً مع كافة الأجهزة. ولذلك كان ينبغي أن يكتب بلغة كومبيوترية يمكن لجميع أنواع المعالِجات تعديلها، وكما يعلم المبرمجون فإن اللغة التي تلبي هذه الحاجة على أفضل وجه كانت لغة البرمجة سي C، ولحسن الحظ، أن زيمرمان كان يتقن هذه اللغة تمام الإتقان. كذلك يجب أن يكون البرنامج سهل الاستخدام، واسع الانتشار ومتاح في كل مكان وفي جميع الأوقات تقريباً، ويسهل فهمه بسرعة. وهكذا يصبح بإمكانه الإفادة من تأثير الشبكة.

كان شارلي ميريت يشكِّل عائقاً إذ لم يسبق له أن تعامل مع لغة البرمجة سي، لكنَّه كان قوياً في مجال كان زيمرمان ضعيفاً فيه على نحو يحمل على الأسى: وهو الرياضيات المعقدة التي تسمح للمرء بالتعامل مع الأعداد الضخمة التي تتطلبها خوارزمية رسا. وكان ذلك ضرورياً على نحو خاص لتطبيق الرسا على الكومبيوتر الشخصية، التي تستخدم «كلمات» مؤلفة من 8 بتات في حساباتها: وكانت العملية التي تنطوي على الكثير من التحدي هي تطبيق تلك الأعداد الصغيرة نسبياً، بطريقة يمكن بها معالجة الأعداد الضخمة التي تتطلّبها الرسا ـ والتي تصل إلىٰ 512 بت، و1028 بت، أَو حتَّى أكثر من ذلك. وإذا لم تستطع القيام بذلك على نحو فعَّال، فإن البرنامج سيعمل ببطء شديد لدرجة أن أحداً لن يُقبل على استخدامه.

على الرغم من أن الاتِّصال الهاتفي، الذي أجراه ميريت بشركة ميتامورفيك لم يؤد إِلىٰ اتفاق تجاري فوراً، إِلاَّ أن المكالمات الهاتفية بينه

وزيمرمان، باتت أمراً مستمراً، وكان زيمرمان لا ينفك يسعى، للحصول على كل ما لميريت من معرفة بالداول (التوابع) الحسابية المتعدِّدة الدقيقة. وكانت عملية معقَّدة لدرجة أنَّهما قرَّرا ضرورة قدوم ميريت لزيارة زيمرمان في بولدر في شهر تشرين الثاني/ نوفمبر 1986، وذلك لإقامة ما يشبه المعسكر يكرسانه، لدراسة المسائل الرياضيَّة بشكل مكثَّف.

ولقد كان أسبوعاً حافلاً بالأحداث، ولم يقتصر على الحساب الذي تعلمه زيمرمان. ذلك أن ميريت كان يعمل على مشروع لحساب البحرية، وهو إنتاج شيفرة تقليديَّة؛ قام بتعليمها للشاب الأصغر منه [زيمرمان]. وكان ميريت قد تعاقد بشأن هذا المشروع من الباطن، مع شركة كان يقدم لها المشورة؛ وكانت هذه الشركة هي شركة آر إس إيه داتا سيكيوريتي. وكان قبل سفره إِلىٰ بولدر، قد اتصل هاتفياً بمديرها الجديد ليسأله عن إمكانية اجتماعهما في كولورادو، وهو مكان يسهل الوصول إليه، أكثر من فايتفيل بولاية أركنساس. فوافق جيم بيدزوس على ذلك.

كان بيدزوس يتطلع إِلىٰ عشاء للتعارف بميريت مشحون بالانفعال، رجلان في مطعم يقدِّم شرائح لحم البقر، وهما يدخنان ويتبادلان الأكاذيب. إِلاَّ أنه عوضاً عن ذلك وجد رجلاً ثالثاً انضم إِلىٰ الاجتماع، وهو زيمرمان. وعوضاً عن مطعم يقدِّم شرائح اللحم انتهى بهم المقام في جود إيرث (الأرض الطيبة)، وهو متجر ضخم، تسطع فيه الأضواء ويقدِّم مختلف أنواع السلطة والبقول.

إن الحديث الذي جرى في المطعم أصبح لاحقاً موضع خلاف. وقال جيم بيدزوس فيما بعد أنه فوجئ عندما تحدَّث فيل زيمرمان عن خطته لابتكار برنامج يستخدم أَنظمة تملكها شركة آر إس إيه. وفي الواقع كان لدى الشركة برنامجاً مشابهاً، كان بيدزوس يحمل معه نسختين عنه، ويدعى ميلسيف (البريد الآمن)، كتبه رايفست وأدليمان، الضليعان بالرياضيات والكريبتوجرافيا

ومعرفتهما بهذين الموضوعين تفوق بمراحل، ما استطاع زيمرمان الحصول عليه من ميريت خلال سنتين. ادَّعى زيمرمان أن بيدزوس أُعجب كثيراً بخططه، لدرجة أنه منح المبرمج رخصة، للحصول على الخوارزمية رسا مجاناً. وقد أنكر بيدزوس لاحقاً، وبأعلى صوته أنه قدَّم عرضاً كهذا.

لم ير زيمرمان أي مبرِّر لعدوله عن خططه، فأمضى السنوات القليلة التالية، في توسيع معرفته بالكريبتوجرافيا بحيث يتمكَّن من إتمام برنامج التشفير الخاص به. وكتب بعضاً من أفكاره في بحث نُشر في مجلة IEEE Computer، وهي مجلة مختصة بعلوم الكومبيوتر ذات مكانة رفيعة، وكان ذلك مدعاة لفخر زيمرمان، وهو نجاح يعتد به، لشاب تخرج من جامعة فلوريدا أتلانتيك.

وبعد ذلك، بدأ بالعمل لوضع البرنامج ذاته. ومن الخطوات الهامَّة والحسَّاسة التي قام بها إنتاج خوارزمية التشفير الإجمالية التي تقوم بتحويل نص الرسالة إلىٰ رموز. وتحاشياً لاستخدام معيار تشفير البيانات ومعيار آر سي ـ 2 RC-2 الذي تملكه شركة آر إس إيه واخترعه رون رايفست، أقدم زيمرمان على سلوك طريق محفوف بالمجازفات، وهو إنتاج الشّيفرة الخاصة به. وكانت مبنية على الشّيفرة التي علمه إياها ميريت، تلك الشّيفرة التي ابتكرها هذا لصالح سلاح البحرية. لكن زيمرمان جعل النِّظام أكثر متانة عن طريق تقديم حلقات متعدِّدة من الاستبدالات. وبينما كان يعمل على صقل فكرته، تذكّر فقرة قام بأدائها دان آيكرويد في برنامج تلفزيوني يدعى ساتردي نايت لايف (البث المباشر ليلة السبت). وهذه الفقرة تمثّل بائعاً جوالاً من الباعة الذين يعملون آخر الليل تتدافع الكلمات من فمه رشاً، وكان آيكرويد ينادي على خلاط قوي جداً لدرجة أن بإمكانك أن ترمي بسمكة فيه، وسيكون السائل الناتج عبارة عن عصير مفيد للصحة (يا لمذاقه اللذيذ). كان اسم ذلك الخلاط باس ـ او ـ ماتيك، فقال زيمرمان لنفسه، يا له من اسم مثالي لخوارزمية تشفير، إن أي

محلّل للشيفرة يواجه رسائله المعماة، لا بدّ عاجز عن توضيحها، كما أمل، مثله في ذلك مثل من يحاول انتشال سمكة فضية اللون ضربت بقوة من المصيدة التي أنتجها خلاّط باس ـ او ـ ماتيك.

انتقل زيمرمان للاهتمام بمشكلات أخرى، استطاع حلّها جميعها كتنظيم الرسالة والسطح البيني ومجموعة من البروتوكولات. ولكن كل ما كان لديه بعد أشهر عديدة من العمل، مجموعة من المكونات منفصلة عن بعضها البعض، ولا تزال غير مترابطة، لا يجمعها برنامج عامل. وقد قال عن ذلك: «إن ربط هذه العناصر ببعضها البعض، يتطلّب عملاً وجهداً عظيمين». وبحلول عام 1990 ـ أي بعد ستّ سنوات من الزيارة التي قام بها ميريت إلىٰ بولدر. أدرك زيمرمان، أن عليه لكي ينجز مشروعه، أن يلتزم به التزاماً كاملاً، حتّى ولو كان ذلك يعني التقشف وضبط الميزانية، وأن يتوقف عن قيامه بتقديم المشورة، وقضاء وقت أقل مع أسرته. وباشر العمل بالبرمجة فوراً منقطعاً له ساعات طوال.

كان زيمرمان قد فكّر بإطلاق اسم معين على العمل الذي يقوم به لكن ليس اسماً رناناً بلا وقار مثل باس ـ او ـ ماتيك. وكان زيمرمان من أوائل الرواد المخلصين لكومبيوترات ماكنتوش، وسبق له أن جرّب وضع برنامج بسيط لاتّصالات البيانات، حين لم يكن قد ظهر أي منها بعد. وفيما كان يفكر خطر بباله Ralph's Pretty Good Grocery، العراب الخيالي في البرنامج الإذاعي A Prairie Home Companion الذي يخرجه جاريسون كيلور، ثم خرج باسم Pretty Good Terminal «محطة طرفية جيدة جداً» وقاده هذا إلىٰ تسمية برنامجه للشيفرة Pretty Good Privacy «منتهى السرِّيَّة» [أصبح يُعرف بالاسم المختصر P.G.P. هـ. م]. والحق أنّه لم يكن ليفكر جدياً بأن هذا الاسم يصلح لأن يكون علامة تجارية كبيرة. ولكن أي ضير في هذا، فلطالما كانت مشاريعه التجارية مشوبة بالغموض. وكان يأمل في جني بعض المال، من بيع برنامجه منتهى السرِّيَّة،

بي جي بي .P.G.P لكنَّه قدر أن الريعية ستكون متواضعة ذلك أن البيع سيكون وفق قواعد الحصول، على حصة من السلعة، وبموجبه يقوم الناس بتصريف البرنامج ويسدِّدون الثمن، بموجب نظام الدفع عند الاستحقاق.

دأب زيمرمان على العمل طوال الأشهر الستة التالية، اثنتي عشرة ساعة يومياً في غرفة نوم في منزله، الذي كاد أن يخسره لأنه لم يكن لديه المال لتسديد أقساط الرهن. ولعله اعتقد، أنه حينما ينهي برنامجه ويطلقه في السوق، فإن أعداداً لا بأس بها من المستثمرين لهذا البرنامج سوف يرسلون له المال مما يمكنه من حل مشكلاته المادية. ولما شارف البرنامج على الانتهاء اتصل بجيم بيدزوس ليرى إذا كان بإمكانهم أخيراً تسوية موضوع الملكية الفكرية التي تطرّق إليها مدير شركة آر إس إيه خلال ذلك العشاء المشؤوم. وشرح له زيمرمان منتجه وطلب منه الإذن باستخدام الخوارزمية رسا. فدُهش بيدزوس لذلك الطلب: هل يعتقد هذا الرجل، أننا سنقدم له أغلى ما عندنا على طبق من فضة. وأشار على زيمرمان أنه ربما كان من الأجدى له، تصنيع منتجه لصالح إحدى الشركات الغنية التي تستطيع أن تحصل على ترخيص رسمي من شركة آر إس إيه، بدلاً من التسول.

كانت المحادثة برمتها، بعيدة كل البُعد عن رؤية زيمرمان لمُنتَجه، ونظرته القاتمة لعالم التجارة الضخمة، لدرجة أنَّه أشاح عن المشكلة بأكملها، وانصرف إلىٰ عمله من جديد.

ولما أطل عام 1991، كان زيمرمان يحرز تقدماً نحو تصنيع منتج نافع. ثم وقع ما جعله يسلك طريقاً غير الذي سلكه ـ وليجعل برنامج منتهى السرِّيَّة شهيراً. كان العامل غير المتوقع في هذا التحول، هو السيناتور جوزيف بايدن، رئيس اللجنة التشريعية في مجلس الشيوخ ومن المساعدين في اقتراح التشريع المنتظر المتعلق بمكافحة الإرهاب وهو مشروع قانون مجلس الشيوخ رقم 266.

ففي مسودة المشروع المقدم في 24 كانون الثاني/ يناير، أدخل بايدن لغة جديدة:

إن الرأي السائد لدى الكونغرس، أن على القائمين بتأمين خدمات الاتِّصال الإِلكترونية ومصنعي تجهيزاتها، ضمان أن تمكن أَنظمة الاتِّصالات الحكومة من الحصول على النّص الواضح لمحتويات الصوت، والبيانات، ووسائل الاتصال الأخرى، عندما يتم إقرار ذلك قانونياً. [إضافة التشديد].

كانت هذه إبرة مسمومة، في كومة قش من البنود والفقرات والقيود، ومع ذلك فقد أفلت هذا المقطع من التدقيق والتمحيص. لكن ظهوره لم يكن محض صدفة. ولا بد أن تكون لغة مشروع القانون، قد صيغت بمساعدة المؤسّسات التي تعمل على حفظ النظام. وتم وضع هذه الجملة بناء على طلب صريح من مكتب التحقيقات الفيدرالي FBI. ويا لها من جملة! فلقد كانت بمثابة طعنة خنجر في قلب ثورة الشّيفرة. فكيف يمكن لشركات التكنولوجيا والخدمات أن تعد بتقديم محتويات النصوص الواضحة للنصوص المشفّرة إذا استخدم الناس لتشفيرها برامج مثل ميلسيف ولوتس نوتس وبي جي بي؟ فالرسائل الأصلية يراد بها أن يقرأها المتلقي المقصود. ومنطقياً، الطريقة الوحيدة التي يمكن بها إرضاء «الرأي السائد في الكونغرس» هي حظر جميع برامج التشفير، فيما عدا تلك المزودة «بالأبواب السرّيّة» التي بإمكان المصنعين والقائمين على الخدمات فتحها نزولاً عند طلب السلطات الفيدرالية.

ولكن، لم يعلم العاملون في مجال الشيفرة بهذا التشريع ـ الذي يعد قنبلة موقوتة ـ إِلاّ بحلول نيسان/ أبريل من عام 1991. إذ كشف مستشار كان يعمل لدى وكالة الأَمن القومي عن هذه الفقرة المسيئة في عدة لوحات لنشرات الإنترنيت، ومعها تعليق رؤيوي: «هل بين قراء هذه القائمة من يعتقد بأن القائمين على تأمين خدمات الاتصالات الإلكترونية، يستطيعون الاحتفاظ

لأنفسهم بالقدرة على قراءة جميع الاتّصالات، وكذلك الإبقاء على «سرِّيَّة» الاتّصالات بأي معنى من المعاني؟... إن أي تأكيد بأن كل استخدام لأي من الأبواب السرِّيَّة، سيكون عندما يقر قانونياً بشكل مناسب وحسب، إنما هو هراء... وأي آلية كهذه ستكون عرضة لإساءة الاستخدام. وانتهت الرسالة بتحذير، عمل على جرف فيل زيمرمان مع التيار: «إني أقترح أن تبدؤوا بتخزين معدات التشفير، وهي ما تزال في متناولكم».

كان مشروع قانون مجلس الشيوخ اس 266، هو الموعد النهائي بالنسبة لفيل زيمرمان. فإذا لم يستطع إخراج برنامجه الجديد بي جي بي إِلىٰ العالم الآن، فإنه قد يُواجه بحظره من الحكومة. وفي الوقت الحالي على الأقل كان التشفير داخل الولايات المتّحدة لا يزال قانونياً. لذلك قرَّر زيمرمان أن ينهي النسخة الأولى من برنامجه بسرعة ويجعلها متاحة لأكبر عدد ممكن من الناس. كذلك تخلّى عن الآمال التي عقدها بجني الأرباح من برنامجه «منتهى السرِّيَّة». فعوضاً عن إصداره كسلعة محصصة جعله سلعة متاحة مجاناً. ولم يكن ذلك يعني أن البرنامج لن يكلف شيئاً فحسب، بل يعني كذلك أن بإمكان المستثمرين توزيعه بأنفسهم شرقاً وغرباً بمباركة مبتكرة.

ولحسن الحظ، أنه وجد واسطة سهلت تداول برنامج مثل منتهى السرِّيَّة، أكثر من أي وقت مضى في التاريخ: وكانت تلك الواسطة هي الإنترنيت. ففي عام 1991 كانت شبكة الكومبيوتر، التي كانت ملكاً للدولة سابقاً في بداية انتشارها السريع الخاطف في كل مكان وجميع الأوقات. إذ راحت تعج بالآلاف من حلقات النقاش، وتحمل ملايين الملفات يومياً. لكن غالبية المستثمرين في ذلك الوقت لا يمثّلون الناس بشكل عام، فمعظمهم كانوا من العارفين بالكومبيوتر والكثير منهم جريئون إِلىٰ أبعد الحدود. غير أن هؤلاء كانوا من النوعيات ذاتها التي ستستجيب لـ بي جي بي الذي كان على الرغم من جهود زيمرمان الحثيثة، لا يزال استخدامه دون برامج مثل ماك رايت، أو تيتريس يسراً، وسهولة في الاستخدام.

والأمر الغريب، في ذلك الوقت، أن زيمرمان، لم يكن من المتحمسين للإنترنيت. وعرف استخدام البريد الإلكتروني بصعوبة، وهو بهذا المعنى كان لا يزال الغريب الذي ينظر إلىٰ الداخل. لكنه في الأشهر الأخيرة، أخذ يراسل شخصاً من المتحمسين للتشفير يعيش في كاليفورنيا، يدعى كيلي جوين، تعرف إليه من خلال شارلي ميريت. ويبدو أن زيمرمان في غضون شهر بعد الاتّصال الهاتفي الذي أجرياه بخصوص مشروع قانون مجلس الشيوخ إس 266، قد قدم نسخة من برنامج منتهى السرِّيَّة، لينتشر عبر الإنترنيت، وكتب زيمرمان لاحقاً عن ذلك «مثل بذور الهندباء البرية». وفي 24 أيار/ مايو قام جوين بإرسال رسالة عبر البريد الإلكتروني إلىٰ جيم وارين، وهو ناشط في مجال الكومبيوتر وله زاوية في صَحيفة مايكرو تايمز المختصة في شؤون الكومبيوتر والمنتشرة في منطقة الخليج (سان فرانسيسكو)، وشرح له الهدف من إغراق الشبكات ببرنامج منتهى السرِّيَّة. وكتب جوين قائلاً: كان ذلك لنسف الحجّة التي تقوم عليها فقرة ما يسمى بالباب السري في مشروع قانون مجلس الشيوخ الجديد قبل إقراره». وبتعبير آخر، إذا كانت الآلاف من نسخ برنامج «منتهى السرِّيَّة» باتت تستخدم، فسيعتبر مشروع القانون إس 266 غير مجد؛ فعندما تواجه الشركات الكبرى للاتّصالات أمثال إيه تي أند تي AT & T بملفات مشفَّرة بواسطة برنامج منتهى السرِّيَّة، ستكون عاجزة عن ضمان النص الصريح لرجال المخابرات أو الأشباح.

وفي عطلة نهاية الأسبوع من شهر حزيران/ يونيو، تلقى جيم وارين عدداً من الاتّصالات من جوين، الذي أخبره أن يوم منتهى السرِّيَّة قد حل. ومن الواضح أن جوين كان مسحوراً بتأثير الحوادث بمجملها، واتخذ تدابير احترازية، مستوحاة من كتاب ماكسويل سمارت أكثر مما استوحيت من جيمس بوند. وكتب وارين فيما بعد في مايكرو تايمز: «كان يتجول بسيارته حول منطقة الخليج ومعه كومبيوتر نقال ومولف أصوات وهاتف خليوي، ويتوقف عند

هاتف عمومي، ويقوم بنقل عدد من النسخ لبضع دقائق، ثم يقطع المكالمة ويهرع إِلىٰ هاتف آخر يبعد أميالاً. إذ قال أنه يريد أن ينشر أكبر كمية ممكنة من النسخ وعلى أوسع نطاق ممكن من البلاد قبل أن تتمكّن الحكومة من الحصول على أمر قضائي بمنع نشره».

ويبدو أن جوين كان حريصاً على نقل البرنامج إِلىٰ مواقع الإنترنيت داخل الولايات المتّحدة فقط. ولكن بالطبع، ما أن يظهر برنامج على مخدم ملفات الشبكة، حتّى يكون بإمكان أي شخص في العالم تخزينه: متسلّلون باكستانيون أَو إرهابيون عراقيون، أَو بلغار ثائرون، أَو زناة سويسريون، أَو طلاّب مدارس ثانوية يابانيون، أَو رجال أعمال فرنسيون، أَو هولنديون يعملون في مجال صور الأطفال الإباحية، أَو نرويجيون مهووسون بالخصوصية، أَو تجار مخدرات كولومبيون. وعلى الرغم من أنه لم يصبح بعد متداولاً على نطاق واسع، فإن شعار الإنترنيت بدأ يصبح مألوفاً: إن الحدود على طريق المعلومات الدولي لم تعد سوى صدمات ناتجة عن السرعة.

ما هو مبلغ السرعة التي غادر بها برنامج بي جي بي الولايات المتّحدة ووجد طريقه إِلىٰ ما وراء البحار، حتّى دون أن يتوقف للسلام على قوانين التصدير؟ فوراً. وقد دهش زيمرمان حين بلغه في اليوم التالي، أن الناس في دول أخرى، يشفرون رسائلهم بواسطة بيانات بي جي بي. كيف يمكن لزيمرمان أن يتجنّب هذا العبور غير القانوني لبرنامجه إِلىٰ دول بعيدة؟ وقد كتب لاحقاً: «كان من الممكن ألا أنشره إطلاقاً، لكن ليس ثمة قانون يحول دون حصول الأمريكيين على كريبتوجرافيا منيعة». فبعد كل شيء لقد دبر زيمرمان نشره المفاجئ لبرنامجه بي جي بي ليس للاحتيال على قوانين التصدير، ولكن لتسليح رجال بلده، الناس الذين ربما يتضرَّرون من مشروع قانون مجلس الشيوخ رقم 266. لقد كان شعاره، كما عبّر عنه في توثيقه للبرنامج: عندما يكون التشفير محظوراً، فإن الخارجين عن القانون وحدهم سيحصلون عليه».

ومن قبيل المفارقة، أن اللغة المهينة التي استخدمها جوزيف بايدن، وكانت الحافز لزيمرمان، ليخطو خطوته الخارقة، لم تلق الحماس الذي حظي به برنامج منتهى السرِّيَّة. ولقد فوجئ السيناتور بايدن بالغضب الجماهيري الهائل (الذي أزكته جماعات الحريات المدنية) بسبب اللغة المعادية للسرِّيَّة والخصوصية التي استخدمها. وبحلول شهر حزيران/ يونيو، قام بسحب هذه الفقرة بهدوء. لكن الحادث خلف تركة غير متوقعة: مئات الآلاف من الرسائل المشفَّرة ببرنامج «منتهى السرِّيَّة» يتم تداولها في مختلف أرجاء المعمورة. لقد أفلت برنامج «منتهى السرِّيَّة» من السواقة الصلبة لكومبيوتر فيل زيمرمان وتمّ استنساخه بأعداد تنأى عن الحصر. ولم تعد قدرته على استرداده أكثر من قدرة المرء على استرداد الكلمات بعدما خرجت من شفتيه.

كان زيمرمان فخوراً ببرنامجه PGP 1.0 بي جي بي 1,0، بالرغم من أنّه كان في موقع الدفاع بسبب عيوبه. كون البرنامج لم يأت بفتح رياضي جديد. ولربما كان الترميز سيء التنظيم حتّى أنّه شعر بضرورة الاعتذار عنه في وثائقه. لكنّه كان واحداً من أوائل الحلول العملية التي أتت بها الكومبيوتر الشخصية ويمكن استخدامها لنظام كريبتوجرافي كامل، بدءاً من التواقيع الرقمية إلىٰ التشفير. وفي ذلك يقول: «إذا ما نظرت إلىٰ ما كان متوفراً في ذلك الوقت، لم تجد إلاّ نسخاً معدّلة تجريبية عن خوارزمية رسا. نشرت إحداها في مجلة بايت Byte؛ ورأيت أن القيام بحسابات خوارزمية رسا يستغرق عصر يوم بكامله. أما برنامجي فلم يكن يتطلّب سوى ثوان لإنجاز مثل ذاك العمل. إنني ابتكرت تطبيقاً عملياً يحتوي على كل ما تحتاج إليه لوضع كريبتوجرافيا المفتاح العام. لقد كان حدثاً هاماً. . . حدثاً فاصلاً».

لكن شخصاً واحداً عارض ذلك بشدَّة، هو جيم بيدزوس مدير شركة آر إس إيه وشركة ببليك كي بارتنرز. فعندما رأى برنامج بي جي بي، ثارت ثائرته. إذ شعر أنّه لم يكن مُنتَجاً أصيلاً وإنما سرقة واضحة لتقنيات شركته،

وبراءات اختراعاتها ـ حسبكم أن تنظروا إِلىٰ ميلسيف ـ فلماذا لم يكن زيمرمان أميناً وأطلق عليه اسم منتهى السرِّيَّة؟ اتصل بيدزوس بالمبرمج، الذي يعيش في كولورادو ـ صارخاً به ـ وطالبه بسحب البرنامج من التداول. فعلى الرغم من العدائية التي كان بيدزوس يحملها في الماضي، فوجئ زيمرمان بهذه الاستجابة، وقال: «اعتقدت أنه سيكون مسروراً». وحاول الدفاع عن نفسه، بأنَّه قام بوضع بي جي بي لأسباب سياسيَّة، وليس ليتحدَّى أي مشروع تجاري. فبعد كل شيء، إن الخمسمئة شركة التي تذكرها مجلة فورتشن وتعتبر زبائن آر إس إيه المحتملين لا يستخدمون سلعاً مجانية؛ بل يشترون برمجياتهم من شركات تدعمها وتساندها. إذن، ما المشكلة؟

لقد اتهمه بيدزوس بأنه ألعوبة في يد وكالة الأَمن القومي، ذلك أن كل ما يضرّ بشركته كان يسعد فورت ميد.

وبعيد ذلك، طلب بيدزوس من محاميه توجيه إنذار لزيمرمان لأنه بعمله هذا، ينتهك براءات اختراع ببليك كي بارتنرز. وهذا أقلق زيمرمان فاتصل ببيدزوس ثانية، محاولاً عقد صفقة معه. وكان أساس الاتفاق بسيطاً: عدم قيام زيمرمان بتوزيع برنامجه مع بروتوكولات رسا، وبالمقابل لا يقاضيه بيدزوس. وبالفعل تمّت صياغة اتفاق بهذا المعنى، وقام زيمرمان بتوقيعه. لكن كل فريق كان له فهمه الخاص لهذه المحادثة الهاتفية. شعر بيدزوس أن الاتفاق أرغم زيمرمان عملياً على قتل بي جي بي. وأصرّ زيمرمان على أنَّه إنما أكَّد فهمه لاتفاق افتراضي ليس إِلاَّ، ومؤداه أنَّه إذا توقف عن توزيع برنامج بي جي بي، فإن الطرف الآخر يمتنع عن ملاحقته قضائياً. كذلك يدعي زيمرمان أن بيدزوس أعطاه تأكيداً شفهياً بأن شركة آر إس إيه ستقوم ببيع تراخيص لمستثمري بي جي بي النهائيين، وذلك ليصبح بإمكانهم استثمار البرنامج دون أن يكون في ذلك انتهاك لبراءات اختراع آر إس إيه. لكن بيدزوس أنكر هذه الإدعاءات.

اتضح لاحقاً أن تفسير زيمرمان لـ «توزيع بي جي بي» كان ضيقاً بعض

الشيء. وشعر أنّه بترك أمر التوزيع للآخرين يصبح حراً ليتفرّغ للبرنامج. وفي الواقع، فإن زيمرمان كان يشرف في تلك الأثناء، على الإصدار الثاني لبرنامج بي جي بي، بمساعدة بعض الاختصاصيين بالشيفرة الأوسع خبرة.

أدرك زيمرمان أنه بحاجة للمساعدة بعد تجربة إعادته إلىٰ صوابه في مؤتمر كريبتو 91 في سانتا بربارة. وكانت مهمته الرئيسة الحصول على استطلاع رأي العلماء البارعين هناك، حول جانب الأمان في برنامج منتهى السرِّيَّة. (مع الإقرار بأنّ هذا كان أمراً تأخر كثيراً، باعتبار أن آلاف الأشخاص باتوا يستخدمون البرنامج. وعلى الفور هرع إلىٰ براين سنو، وهو واحد من كبار علماء الرياضيات والمختصّين بالشيفرة في وكالة الأَمن القومي. وبالطبع كان زيمرمان يشعر بالفضول لمعرفة إن كانت الحكومة مستاءة من برنامج بي جي بي. لكن سنو قال له: «لو كنت مكانك، لخشيت من ملاحقة جيم بيدزوس لي قضائياً أكثر من خشيتي من الحكومة».

ولقد أثار هذا حيرة زيمرمان، فلماذا لم تكن الحكومة قلقة؟ ثم سعى للحصول على تعليقات خاصَّة على برنامجه. وفي بادئ الأمر صرفه آدي شامير الكريبتوجرافي الإسرائيلي، وبعد ذلك قال له أن يرسل البرنامج إلىٰ إسرائيل وسيمضي عشر دقائق في دراسته، لكن زيمرمان استحوذ على اهتمام إيلي بيهام زميل شامير في معهد وايزمن. وانتجع الاثنان إلىٰ كافتيريا جامعة كاليفورنيا في سانتا بربارة، التي كانت مسرحاً للكثير من السجالات الأشبه باشتباك قرون الثيران وتحليل الشّيفرة الارتجالي في المؤتمر السنوي لعلماء الشّيفرة. وبالنسبة لزيمرمان، كان غداء طويلاً بأكثر من معنى، إذ سرعان ما أحرج بيهام ذلك الكريبتوجرافي الهاوي حينما كشف له عيوباً ذات شأن في برنامج باس ـ أو ـ ماتيك، فعلى سبيل المثال، كانت الشّيفرة ضعيفة أمام هجوم تحليل الشّيفرة التفاضلي. وفي حين أن باس ـ أو ـ ماتيك لم يكن برنامجاً ميؤوساً منه، إلاّ أنه أبعد ما يكون عن كونه كنزاً ثميناً.

أدرك زيمرمان الآن أن الطريقة الوحيدة التي يمكنه بها تطوير برنامجه منتهى السرِّيَّة هي أن يعرف حدود إمكاناته. وأن أعظم إنجاز له في مجال ابتكار الرموز يتحقَّق بإدراكه أنَّه ليس بالكريبتوجرافي العظيم، وإنما واضع رزم ومبرمج واسع الاطلاع لبرامج عادية وتطبيقيَّة عامة. لكنَّه يحتاج إِلىٰ مختصين في الرياضيات والكريبتوجرافيا من طراز رفيع ليساعدوه في التفاصيل الجوهرية الصعبة.

ومن حسن الحظ، أن العديد من الأشخاص الأذكياء قد أزكى الحماس لديهم صدور برنامج بي جي بي 1,0. وعوضاً من أن تضايقهم نقاط ضعفه، كانوا توَّاقين للمساهمة والعمل على إصلاحها. وسرعان ما جنّد زيمرمان متطوعين من نيوزيلندا وهولندا وكاليفورنيا ليصبحوا المهندسين الذين يعتمد عليهم. كذلك اجتمعت له جماعة من الفضوليين على غير اتفاق فقدَّموا له النصيحة وبضعة قطع صغيرة. وبدأوا جميعاً بالعمل معاً على إصدار النسخة 2,0 من برنامج منتهى السرِّيَّة. وكان زيمرمان المصمِّم الأساسي، وهو القائم على كل قرار وكل من الرموز، إلاَّ أنه حرص على إخفاء دوره، لئلا يعتقد بيدزوس، أنَّه نكث عهده بألاَّ ينتهك براءات الملكيَّة الفكريَّة لآر إس إيه.

كانت النتيجة برنامج بي جي بي 2.0 PGP 2.0، وكان مُنتَجاً أقوى مما سبقه إِلىٰ أبعد الحدود. وهذا نحَّى برنامج باس ـ أو ـ ماتيك جانباً (ويقول زيمرمان: «إن إطلاق اسم كهذا عليه لم يكن فكرة حسنة، على أي حال. فالكريبتوجرافيا أمر لا يمكنك الاستخفاف به»). وعوضاً عنه، اختار زيمرمان شيفرة سويسرية أقدم، تدعى خوارزمية تشفير البيانات الدولية أَو IDEA آيديا. وضعها اثنان من مشاهير علماء الرياضيات المختصين بالشّيفرة وذلك في عام 1990، وسرعان ما أثبتت آيديا وجودها أمام تمحيص الجماهير. وشعر زيمرمان أن شيفرة آيديا كانت أقوى من معيار تشفير البيانات ديز، وخاصة مع مفاتيح 128 ـ بت التي أوصى بها. وفي توثيقه للإصدار 2,0 كتب: «إن هذه ليست بخوارزمية مصنّعة محلياً».

وكان ثمة تطوير آخر، في ناحية كان زيمرمان تجاهلها أساساً، في برنامجه بي جي بي 1,0: توثيق المفتاح، وهي العمليَّة التي يتم فيها التثبّت من المفتاح العام. وغالباً ما كان يُنظر إلىٰ التوثيق على أنَّه عقب أخيل (نقطة الضعف) في أَنظمة المفتاح العام. ويظهر اللغز التقليدي في مثل هذه الأَنظمة عندما تريد أليس أن ترسل رسالة لبوب. فتعمل على تشفيرها بمفتاح بوب العام، وليس بإِمكان أحد أن يفكّها، سوى بوب. لكن ماذا لو أن أليس لم تلتق ببوب من قبل، فكيف لها أن تحصل على المفتاح العام لبوب؟ إذا سألته عنه مباشرة، فليس بإمكانها أن تشفِّر طلبها (من الواضح أنها لا تستطيع، فمفتاحه العام ليس لديها بعد، والذي ستستخدمه لتشفير الرسالة). لذا فإن متنصتاً محتملاً، مثل إيف، يستطيع أن يؤدي دور «رجل في الوسط» ويختطف الرسالة في الطريق. عندئذ سترسل إيف ـ مدعية أنَّها بوب ـ مفتاحها العام إلىٰ أليس زاعمة أنَّه مفتاح بوب. (يعرف هذا التنكّر المضلّل بـ «الخداع») فإذا خُدعت أليس، فستشفّر رسالتها السرِّيَّة إلىٰ بوب باستخدام ذلك المفتاح. واحسرتاه، فلن يكون بوسع بوب فهم تلك الرسالة التي شفَرت بذلك المفتاح، بل هي إيف المخادعة وحدها بإمكانها ذلك. وحسبنا هذا من ضمان سرِّيَّة الطلبات المباشرة.

ماذا بشأن نشر ما يشبه دليل هاتف رقمي مليء بأَرقام مفاتيح عامة؟ إن مشكلة الاحتيال تظل قائمة، ما لم يكن لديك وسيلة أمينة يُعتد بها لحماية ذلك الدليل وضمان أن تكون المفاتيح تعود فعلاً لأصحابها المزعومين. أجل إن النجاح في هذه الخديعة يتطلَّب جهداً جباراً. لكنَّه ممكن، وما دامت قابلية الانتهاك قائمة، فإن على أي نظام مفتاح عام أن يجد طريقة للالتفاف على هذه الثغرة الأمنية.

كان الكثيرون يعتقدون أن الحل يكمن في إنشاء «سلطة مُوثِقة» على نطاق واسع لتوزيع المفاتيح العامة والتثبّت من صحتها. إن مركزاً كهذا سيكون قادراً

على معالجة الملايين من المفاتيح العامَّة. وباستخدامك المفتاح العام للسلطة الموثقة، من المفترض أنه مفتاح متداول كثيراً لدرجة أنَّه ما من أحد يستطيع خداعه، بإمكانك أن تستعلم وأنت مطمئن عن المفتاح العام لأحدهم، أَو أن تتأكّد من مفتاح عام أرسل إليك. وبالطبع، فإن حلاً طموحاً كهذا كان مستحيل التحقّق لزيمرمان. ذلك أنَّه لم تكن لديه لا الوسيلة ولا الأموال لإقامة مركز لسلطة موثِقة لمراقبة التوزيع والتحقّق من المفاتيح العامَّة. لذا كان عليه أن يفكّر ويخرج بمنهج آخر.

كان الحل الذي خرج به مبتكراً للغاية. خاصة أنَّه عكس إحساس الغريب الذي كان يميز جهوده. فعوضاً عن إنشاء سلطة مركزية للمفاتيح تصور مجتمع برنامج بي جي بي نفسه هو السلطة. وشرح زيمرمان ذلك في مقابلة أُجريت معه عام 1993، بقوله: «إن برنامج بي جي بي يتيح لأطراف غير المرسل والمستلم، وهم أصدقاء موثوقين من الطرفين، أن يوقعوا المفاتيح. وهذا يثبت أن الرسالة وردت من الأشخاص المعينين أنفسهم». وبقوله «توقيع» المفاتيح، كان زيمرمان يعني بذلك تقنية، يمكن للمرء بواسطتها أن يربط مفتاحه أَو مفتاحها العام بمفتاح شخص آخر، وكأنَّه خاتم بالموافقة. فبعد أن تولد مفتاحاً عامّاً، تعمل على جعل بعض معارفك الشخصيين، يوقع على مفتاحك. ويجب أن تتم هذه التواقيع وجهاً لوجه، وذلك لتقليص خطر الوقوع في الخداع. لذا إذا كانت أليس تعرف بوب شخصياً، فإنَّها ستدبر لقاء معه وتقدم له بنفسها القرص الذي يحتوي على مفتاحها العام، الذي أوجدته باستخدامها برنامج بي جي بي. وباستخدام بوب لنسخته من برنامج بي جي بي، يوقّع بوب المفتاح العام لأليس بمفتاحه الخاص. (يتم ذلك ببساطة بانتقاء دالة في برمجية البرنامج والنقر على الفأرة) ويعيد لها المفتاح الموقّع ويحتفظ بنسخة ليضمها إلى «حلقة المفاتيح العامّة» وهي مجموعة من المفاتيح الموقعة والتي يتم تشجيع مستثمري برنامج بي جي بي على الاحتفاظ بها في السواقة الصلبة الخاصة بهم. وقد

يرغب، فيما بعد، فريق ثالث، ولتكن كارول، في التخاطب وأليس، إلاَّ أنها لا تعرفها. لذا تسعى كارول للحصول على مفتاح أليس العام، إما عن طريقها مباشرة أَو من لوحة إعلانات تحفل بالمفاتيح العامّة. وفي الحالة الثانية كيف لها أن تعرف أنها أليس فعلاً؟ إنها تتوقف لترى من الذي وقّع المفتاح، هل يحمل علامة موافقة شخص تعرفه؟ ولما كانت كارول تعرف بوب، وكانت سابقاً قد تلقت نسخة موثقة من مفتاح بوب العام، لذلك بإمكانها أن تتأكّد من صحة توقيعه. فإن تحقّقت منه، فإن ذلك يعني أن بوب، قد التقى فعلاً بالشخص الذي يحمل هذا المفتاح الجديد، وهو يقول لكارول بكل وضوح: «نعم إنها أليس نفسها». وبإمكان كارول أن تكون واثقة من أن أليس ذاتها. على الأقل، إلىٰ الدرجة التي تثق فيها ببوب.

إن هذا النّظام الذي يُعرف بـ «شبكة الثقة» يحتاج إلىٰ شيء من المحاكمة العقليَّة من طرف المستخدم. فبعد كل شيء، لا يمكن لكارول أن تتأكّد من هوية أليس ما لم تكن هي نفسها تعرف شخصاً ما، كان قد التقى بها شخصياً ووقّع مفتاحها. وماذا لو لم تكن تعرف أحداً وقّع المفتاح شخصياً؟ هل الأمر يستحق الوثوق بإثبات من الدرجة الثانية؟ ربما لم يكن صديقها بوب قد وقّع مفتاح أليس، لكنه كان قد وقّع مفتاح شخص يدعى تيد. وتيد هذا وقّع مفتاح أليس. أما ثقتك بذلك التوقيع، فأمر يعتمد على سمعة تيد: ومن هم الأشخاص الذين وقّعوا مفتاحه؟ ولما كان إقبال الناس على استخدام برنامج بي جي بي في ازدياد، فمن المحتمل أن بعضهم سوف يعرف بأنّه كثير الوساوس بما يتصل بالتحقّق من المفاتيح التي يوقّعها. إن رؤية واحد من هؤلاء المعرفين الموثوقين على حلقة مفتاح سيكون عندئذ إثباتاً على صحته. وعلى أي حال، فإن برنامج بي جي بي يتيح للمستخدمين تحديد ما يشير إليه الكريبتوجرافي بروس شناير بـ «مستويات البارانويا»: أي أن عدد مستويات الفصل، التي أنت على استعداد للقبول بها، يعتمد على درجة وثوقك بالعديد من الموقعين.

ومع وجود شبكة الثقة هذه، وخوارزمية تشفير أقوى، ودارة ربط بينية أفضل، وعدد من التحسينات الأخرى، فإن برنامج بي جي بي 2,0، بخلاف البرنامج الكوميدي المفضل عند زيمرمان الذي يُذاع في عطلة الأسبوع، أصبح جاهزاً للعرض الأول. لا بل إن هذا الجمع من الأعوان الذين قدّموا يد العون للبرنامج أعدّوا له ترجمات للبينيات بلغات كثيرة، لذلك كان بإمكان الناس في جميع أنحاء العالم استخدامه منذ اليوم الأول لإصداره. وفي شهر أيلول/ سبتمبر 1992، قام اثنان من مساعدي زيمرمان بإطلاق برنامج بي جي بي 2,0 على الشبكة في بيتيهما في أمستردام وأوكلاند. وبهذه الطريقة يمكن استيراد البرنامج إلىٰ داخل الولايات المتّحدة، دون انتهاك قوانين التصدير. وسرعان ما خلف الإصدار الجديد الإصدار الأول وفاقه. ويقول زيمرمان: «بعد شهر واحد من الإصدار تلقيت رسائل بريديَّة أكثر بكثير مما تلقيته طوال السنة السابقة. لقد كان الأمر أشبه بالنار في الهشيم».

لقد ازداد جيم بيدزوس غضباً، إذا جاز التعبير، وثارت ثائرته بالأخص، لرأي أورده زيمرمان في الوثائق التي ترافق كل شحنة من برنامج بي جي بي. إذ ادعى زيمرمان أن ببليك كي بارتنرز كانت تنهب الجمهور الأمريكي، بأن جعلت الناس يدفعون ثمن تقنية تم تطويرها بأموال الحكومة. وبعد محاولات زيمرمان تغطية نفسه بالتنصل كقوله: «إن مبتكر هذا البرنامج التطبيقي لخوارزمية رسا يقدم هذا. . . للأغراض التعليميَّة فقط. . . وعلى عاتقك تقع مسؤولية الحصول على رخصة، لاستخدام هذه الخوارزمية من ببليك كي بارتنرز، فأنت المستخدم، وليس فيل زيمرمان. . .»، استرسل في تبرير مطول لأفعاله، مدعياً أنّه لم يعتقد أنّه كان ينتهك حقوق أي براءة اختراع. وألمح إلىٰ أن ببليك كي بارتنرز، بسيطرتها على براءات اختراع كريبتوجرافيا المفتاح العام، فإن هذه الشركة ـ وقد سمّاها «شركة مقاضاة أساساً» ـ كانت تقوم بالأعمال القذرة، نيابة عن وكالة الأمن القومي، وذلك باحتكار التشفير وإنكاره على

الناس عموماً! وأخيراً قال للمستخدمين المحتملين، أنَّه ليس ثمة ما يحملهم على القلق من احتمال خرقهم حقوق براءة اختراع ببليك كي بارتنرز، إذ كتب: «هناك أعداد من مستثمري برنامج بي جي بي أكبر من أن تستطيعوا ملاحقتهم فلماذا ينتقوك للملاحقة دون سواك؟» إلاَّ أنه لم يقدم لهم أي ضمانات.

وفي عام 1994 قال بيدزوس: «إنه [زيمرمان] يضلِّل الناس، ويتعمّد الإساءة إلىٰ سمعتنا لكي يحصل على دعم لبرنامجه. تلكم هي الحكومة الشريرة التي تحاول حرمانكم من حقكم في السرِّيَّة، وأصحاب براءات الاختراع مصمّمون على سرقة أَموالكم ونهب الحكومة، وليس واضحاً من الأسوأ، لكن بإمكانكم أن تصدوهما باستخدام هذا البرنامج. لقد كان يعلم أن [ادعاءاته] زائفة».

كان بيدزوس محقاً في أمر واحد: أنَّه سبق لشركة آر إس إيه أن أنتجت برنامج ميلسيف، وهو تطبيق لبراءات اختراع المفتاح العام. وكان الفريقان كلاهما متفقان، على أن بيدزوس قدم لزيمرمان، أثناء لقائهما على العشاء الذي حصل عام 1986، نسخة من برنامج ميلسيف، لكن زيمرمان يدعي أنَّه لم يختبر البرنامج أبداً، ولم يقرأ الوثيقة المرفقة به، لأنّه كان قد اكتشف طريقة عمل منتجه قبل ذلك. ويقول بيدزوس: «يخبرنا هذا الرجل أنَّه ذُهل لابتكار خوارزمية رسا، ثم يفترض أن نصدّقه حين يقول أنَّه أخذ البرنامج الذي وضعه أصحاب ذلك الإنجاز، وهم أبطاله، ولم يجد لديه الفضول الكافي ليلقي نظرة عليه؟».

لكن معظم غضب بيدزوس، لم يكن موجَّهاً ضد أفعال زيمرمان وحسب، بل إلىٰ الشعبية المتصاعدة لبرنامج بي جي بي أيضاً. لأنَّه كان يقدم مجاناً، وغدا متاحاً في جميع أرجاء العالم بصرف النظر عن قوانين التصدير، ولما اكتسبه من رونق بين جمهور عشَّاق التقنيات المتطورة، فضلاً عن شيوع استخدامه حتى فاق برنامج «ميلسيف»، وأخذ الآن يهدّد بأن يصبح برنامجاً نموذجياً في الإنترنيت. وبالرغم من أن زيمرمان ليس من الكريبتوجرافيين

المبرزين ممن يحملون شهادة من جامعة ستانفورد، ولا ينتسب إِلىٰ الدوحة العطرة لمعهد ماساتشوسيتس للتكنولوجيا، وليست له دراية تقريباً بالتجارة أَو التسويق، إلاَّ أنَّه تمكّن من إنجاز ما عجز عنه علماء الرياضيَّات مبتكرو المفتاح العام ذو الشهرة العالمية، وما فشل فيه جيم بيدزوس الخبير بالسوق: وهو خلف ظاهرة تشفير متصاعدة لم تستمل إِلىٰ جانبها مستثمرين من جماهير الناس فحسب، بل وصفت كذلك بأنَّها التحدي الأكبر للوكالة التي تعمل وراء السياج الثلاثي وتكاليفها التي بلغت عدة مليارات من الدولارات. فلا عجب إن غدا في نهاية عام 1992، بطل النضال السري للشيفرة بعد أن كان مغموراً. ويقول: «لو ذهبت إِلىٰ أوروبا فلن أضطر لدفع ثمن الغداء، إذ لدي أعداد هائلة من المعجبين المتفانين».

كان من شأن جهود زيمرمان الشخصية لابتكار برنامج تشفير وتوزيعه على الناس ـ وهو جهد قام به بهدف الالتفاف على سيطرة الحكومة ـ أن شكَّل بعداً جديداً للمعركة المستمرة بين وكالة الأَمن القومي والكريبتوجرافيين الذين يعملون خارج نطاق سيطرتها. وسبق للوكالة أن شعرت بأن التسويات التي عقدتها مع الأكاديميين لتقديم أعمالهم طواعية قبل النشر قد خففت من معظم المخاطر المحتملة لذلك المجتمع الصاعد. (والخيار هنا ضئيل بسبب التعديل الأول في الدستور) كذلك كان صنائع فورت ميد يعملون أيضاً على إبعاد تهديد التجارة لهيمنتهم بزحزحة موقفهم قليلاً في موضوع التصدير.

لكن الأمر كان يزداد صعوبة في إقناع الناس بأن السيطرة على الكريبتوجرافيا أمر منطقي. إذ أخذ يتضح أكثر فأكثر أن الكريبتوجرافيا لا تنتمي إِلىٰ تكنولوجيا الأسلحة، بل هي تقنية يمكن أن تصبح جزءاً من حياتنا اليومية. لقد كانت هذه الملايين كلها التي تستخدم لوتس نوتس مدركة لمنافعه. وصدم مستخدمو البريد الإِلكتروني المتنوِّع عند اكتشافهم أن الحماية الأساسيَّة لم تكن متوفِّرة في أجهزتهم. إن إرسال البريد عبر الإنترنيت الذي بدا آمناً لكنَّه في واقع

الحال ظلّ متخلفاً خطوة واحدة عن اللحاق بالإذاعة. وعلى سبيل المثال، مع ازدياد أعداد الأشخاص الذين يستخدمون الهواتف الخليوية، راح هؤلاء يتساءلون عما يجعل مراقبة اتّصالاتهم الهاتفية سهلة على أي جهاز فاحص ثمنه مئة دولار. حتى أن المكالمات التي أجراها أمير ويلز مع عشيقته عبر الهاتف الخليوي تم اعتراضها ـ وبسببها أصبح العالم كله يضحك الآن، على كلمات تحبّب قالها لعشيقته ـ كلمات شخصية إِلىٰ أبعد الحدود (حسن، لقد كانت تتعلّق بأشياء تتصل بالطمث). لم لا ينبغي أن يكون كل شيء محمياً، في عالم من الاتّصالات المتطورة جداً؟ فحتى الفريق الوطني لكرة القدم قرَّر التالي: استخدام الشيفرة لتشفير إشارات الراديو التي يرسلها المدرِّبون في غرف المراقبة، إِلىٰ لاعبي الظهير الربعي في الملعب. كان ذلك شيئاً يمكن لأي شخص أن يفهمه. فهناك طريقة بسيطة تمنع فريق جرين باي باكرز من سرقة اللعبة التالية من جون إلواي. . . وندعو ذلك أمنا قومياً؟

تلك كانت أسئلة صعبة، موجهة لفرع من الحكومة ليس معتاداً على الإجابة على أي سؤال إطلاقاً. لكن التساؤل كان على وشك أن يصبح أكثر حدّة، مع دخول قوة جديدة على اللعبة، قوة كان لزيمرمان نصيب في بروزها، وأصبحت الآن فاعلة، إنها الفعالية الكريبتوجرافية Cryptoactivism. أي نشر الكريبتوجرافيا المنيعة عبر الإنترنيت. وحركة ثورية مبنية على إنتاج ونشر وتوزيع الرموز القوية، وقد بدت في ظاهرها نشاطاً عارضاً. لكن مع احتدام الجدل حول التشفير، اتضح أن الوقت قد حان، لظهور حركة صغيرة لتقوم بممارسة بعض الضغط.

هكذا بدا الأمر لاثنين من المتحمسين للشيفرة، خرجا بفكرة إنشاء مجموعة خارج نطاق اللامنتمين في المعركة من أجل الكريبتوجرافيا. ونشأ هذا المفهوم عفوياً عندما قام إيريك هيوز، وهو عالِم رياضيَّات شاب يعيش في شمال منطقة الخليج ويفكّر في الانتقال إِلىٰ جنوب ساحل كاليفورنيا، بزيارة صديقه تيم ماي في سانتا كروز في بحثه عن بيت.

كان هيوز وماي ائتلافاً طريفاً بين شخصين، يجمع بينهما شغف بالعلم، وميول تحررية في السياسة، وقدر من البارانويا غير المثيرة للأعصاب. (كان يحلو لهيوز أن يسخر من هذا، مقتبساً عبارة يفترض أن فيلسوفاً مغموراً كان قد قالها: «إن الكريبتوجرافيا هي النتيجة الرياضية للافتراضات البارانويية»). وكان كلاهما شخصية مؤثرة، طرحا عنهما مظهر عالم الرياضيات، ليرتديا زي رجال الغرب الأمريكي فكانا كريبتو كاوبوي. وغالباً ما كان هيوز، يُشاهد معتمراً القبعة العريضة التي يظهر بها رعاة البقر في الأفلام.

كان ماي فيزيائياً، في الأربعين من عمره، تقاعد قبل سبع سنوات من انتل ومعه كمية من الأسهم. كان إسهامه الكبير في مصنع أنصاف النواقل العملاق برهانه على أن الوقائع الكمية (كوانتوم) ـ حركة الأجزاء المكونة للذرّة ـ يمكن أن تؤثّر في الحسابات التي تقوم بها الرقاقات المصنوعة من أنصاف النواقل. وقد سمح اكتشاف ماي هذا للمصممين في إنتل ابتكار استراتيجيات للتعامل مع هذه المشكلة. مما جعل قانون مور في التقدم المستمر ممكناً. وبعيداً عن التكنولوجيا كان ماي داعية للتحررية في وجه القيود التي تضعها الحكومة. ويقول: «لقد اهتديت لدى قراءتي لكتب آين راند عندما كنت طفلاً، وأثناء الدراسة صرت أكتب مناظرات حول الحقوق الطبيعية». ولما بلغ سن الرشد أرسل مطارحات من هذا القبيل ـ أحاديث صاخبة محرضة عالمياً، ومسلية للغاية ـ إِلىٰ جماعات مستخدمي الشبكة Use net، واكتسب سمعة المنفعل لتأييده الشديد للكريبتوجرافيا المتحرِّرة من كل قيد. وكان ماي رجلاً نحيلاً ذو لحية وغالباً ما كان يرتدي قبعة يعتمر بها أهل الريف النائي، ويمتلك منزلاً صغيراً تتكون فيه أكداس من الكتب والآلات والقطط السمان.

أما إيريك هيوز فكان من طائفة المورمون لكنه شبه مرتد، ومن فيرجينيا، وله لحية طويلة خفيفة ذات لون بني فاتح. ويضع نظارات بإطار معدني، ويتمتع بذكاء لا مبال ساخر. ومع أنَّه لم يكن قد بلغ الثلاثين من عمره إِلاَّ أنَّه

كان ذا شخصية قوية. وكان يلطف من ثقته المفرطة بالنفس ذكاء هادئ يمكنه من فهم وجهي مسألة ما. وكان شغوفاً بالكريبتوجرافيا. ودرس الرياضيات في جامعة بيركلي، وعمل لفترة في شركة في الخارج. والآن مع سطوع فجر الإنترنيت كان يفكّر في كيفية استخدام الرموز لتحصين عصر المعلومات. وهدفه النهائي المزج بين رأسمالية السوق الخالصة والنضال من أجل الحرية. وفي نظرته إِلىٰ العالم، كانت الحكومات تشكل خطراً دائماً على رفاه المواطنين، بما في ذلك الحكومات الرحيمة المزعومة مثل الولايات المتّحدة. ويرى أن خصوصية وأسرار الفرد قلعة تتعرض على الدوام لهجوم الدولة. والمعجزة الكبرى أنه يمكن مقاومة الدولة بالخوارزميات. وفي ذلك يقول: «في الماضي كان المرء يحصل على السرِّيَّة بذهابه إِلىٰ التخوم الطبيعية بعيداً عن الآخرين حيث لا يزعجك أحد. ومع التطبيق الصحيح للكريبتوجرافيا، بإمكانك أن تنتقل ثانية إِلىٰ التخوم وبشكل دائم».

بالرغم من أن رؤى هيوز كانت راديكالية، إِلاَّ أنَّها بهتت بالمقارنة مع رؤية صديقه، الذي يعيش في سانتا روز. عندما فكر تيم ماي في الشّيفرة كان الأمر أشبه بإنزال قطرات من الأسيد. وفي عصر الكومبيوتر، نقوم بخُلق ـ ما يصفه بـ «مناطق افتراضية»، وأن أنابيب وأسلاك المستقبل ـ الملاط والجدران الفعلية لهذه الفضاءات الافتراضية ـ لا يمكن أن يثبتها سوى الشّيفرة وحدها ولا شيء سواها. وعند الحديث عن هذه الرؤى ينفجر ماي قائلاً: «آه، يا إلهي إنها عميقة للغاية. لا يوجد شيء سواها! ويؤكد أن الدوال (التوابع) الوحيدة الاتجاه مثل تلك التي عالجها ديفي وميركل ورايفست، كانت لبنات الفضاء المتخيّل، وإذا لم نستخدمها، فإننا سنتحوّل إِلىٰ كائنات مثيرة للشفقة ترتعش وهي تقف وسط رماد بيت افتراضي محترق. لكن بها يمكن تخيّل كل شيء أقنية ـ لا يمكن لوكالة الأَمن القومي أن تمسّها ـ آمنة من المتسللين في لوس جاتوس، وكاليفورنيا، إِلىٰ الناشطين في سانت بطرسبورج في روسيا. وصفقات بعيدة

عن متناول الضرائب. ونهاية الدولة القومية. كانت تلك هي الثورة القادمة، وفقاً لتيم ماي.

تلك كانت المواضيع التي تمّت مناقشتها في أيار/ مايو عام 1992، أثناء زيارة إيريك هيوز لتيم ماي في بحثه عن المنزل. وكان ثمة الكثير مما يثير الحديث لدرجة أن الحديث استمر بينهما مدة ثلاثة أيام. ويصف هيوز ذلك بقوله: «كنا نستيقظ في الصباح، ويتصل بنا الحديث، غير عابئين بأمر البحث عن البيت المنشود. ثم نذهب لتناول الغداء، ونعود لنتابع الحديث من جديد. واستمر الأمر على هذا المنوال». وبنهاية الزيارة اتفقا على تنظيم اتحاد حر، يتألّف ممن لهم آراء مشابهة ـ لم يحرز هيوز أي تقدم بشأن العثور على منزل، فعاد، ولا عجب، إلىٰ شقته المشتركة في بيركلي ـ كما اتفقا على عدم الجلوس وتبادل الأحاديث غير المجدية، بل على العمل، حسب نهج زيمرمان، على إنتاج الأدوات التي ستسلح الجماهير لمواجهة لصوص الكومبيوتر، ومكاتب القروض، وبشكل خاص الحكومة.

في الأسابيع القليلة التالية، حصلوا على دعم من بعض الشخصيات ذات النفوذ في مجتمع الشّيفرة المعادي للحكومة. وكان أحد الحلفاء الأقوياء جون جيلمور البالغ من العمر سبع وثلاثون عاماً، من متسللي الكومبيوتر لطيف المعشر مسترسل الشعر، في سبيله إلىٰ الصلع، وذو لحية خفيفة. وكان جيلمور قد أصاب ثروة صغيرة بفضل كونه واحداً من المبرمجين الذين يتميزون بالأصالة عندما كان يعمل لدى شيفرة صن مايكروسيستمز ـ كان الموظف رقم خمسة في سلسلة المراتب ـ لكنه ترك العمل عام 1986. وفي عام 1990، قام بتأسيس شيفرة إليكتريكال فرونتير فاونديشن (EFF إي إف إف)، وقد شاركه في هذا كل من ميتش كابور وجون بيري بارلو، والهدف تعزيز الحريات المدنية في العصر الرقمي، وكان قد أسَّس للتو شركة جديدة تُدعى ساينوز سبورت وتهدف إلىٰ مساعدة مستخدمي البرمجيات المجانية. وكانت هوايته المفضلة: السرِّيَّة

الشخصية. وفي مؤتمر عُقد عام 1991 أطلق عليه اسم «الكومبيوتر والحرية والسرِّيَّة» ألقى خطبة استبق فيها أفكار ماي وهيوز ـ حركة تشفير جماهيرية لدرء شر الحكومة.

ماذا لو استطعنا بناء مجتمع لا تجمع فيه أية معلومات؟ مجتمع يمكنك فيه أن تدفع إيجار شريط الفيديو دون أن تترك بطاقة اعتماد أَو رقم حسابك المصرفي؟ ويمكنك أن تثبت أنَّك مؤهل لقيادة السيارة دون أن تعطي اسمك؟ وإرسال أَو تلقي الرسائل دون الإفصاح عن مكان إقامتك، مثل صندوق بريد إلكتروني؟ ذلك هو المجتمع الذي أريد بناءه. أريد أن أثبت ـ باستخدام الفيزياء والرياضيات لا بالقوانين ـ أموراً مثل السرِّيَّة الفعلية للاتِّصالات الشخصية. . . السرِّيَّة الفعلية للسجلات الشخصية. . الحرية الفعلية للتجارة. . السرِّيَّة الفعلية للأوضاع المالية. . [و] السيطرة الحقيقية على الهوية.

كان جيلمور مهتماً بشكل خاص، بأن يكفل وصول المعلومات التي تتحدَّث عن الشّيفرة إِلىٰ عالم الجماهير. (كان هو الشخص الذي استخدم الإنترنيت لنشر البحث الذي وضعه ميركل عن التشفير السريع بعد أن طلبت وكالة الأَمن القومي من شركة زيروكس عدم نشره). وفي العهد القريب، كان يحاول تحرير أربعة كتب مدرسية قديمة في تحليل الشّيفرة، كان قد وضعها وليم فريدمان الرجل الأسطوري البارع في وكالة الأَمن القومي. وتقديم طلبات باسم حرية تدفق المعلومات وذلك لرفع الحظر عن هذه الكتب التي يعود تاريخها إِلىٰ ثلاثين سنة مضت. بل لقد أوكل محامياً في بيركلي، لمساعدته على إتمام العمليَّة المعقدة، ورفع الدعاوى حين لا تبدي الهيئات الحكومية تجاوباً، ضمن الفترة الزمنية القانونية المحدَّدة.

بعيد المطالبة برفع الحظر عن أعمال فريدمان، بدأ جيلمور بحثاً ببليوجرافياً مطولاً حولها على الإنترنيت، مستخدماً برامج «نو بوتز Know-bot» وهي برامج بحث ذكية مؤتمتة. وقد دل البرنامج على توفر نسخ من كتابين

لفريدمان في تفكيك الرموز متاحة لاطلاع القراء، أحدهما في مكتبة كلية فيرجينيا العسكرية، والآخر على مايكروفيلم في جامعة بوسطن. ومن الواضح أن الحكومة قد رفعت عنهما الحظر في وقت من الأوقات، لكن في عهد الرئيس ريغان سُحبا من التداول وأصبحا مرة أخرى من الكتب المحظورة. وعلى الفور حصل جيلمور على نسخ أرسلها إليه أصدقاؤه، وأعلم القاضي الذي ينظر في طلبه بشأن حرية المعلومات أن الكتب كانت متاحة للقرّاء في مكتبات عامة. وكان رد الحكومة إنذار جيلمور، بأن أي نشر آخر لنصوص فريدمان سوف يُعتبر انتهاكاً لقانون التجسّس، الذي ينص على عقوبة بالسجن، لمدة قد تصل إلىٰ عشر سنوات في حال مخالفة أي بند من بنوده. وبعبارة أخرى، يمكن أن يرسل جيلمور إلىٰ سجن ليفنورث مدة عقد كامل، وذلك لمجرد أنَّه أخذ كتاباً من فوق رفوف مكتبة عامة وأطلع أصدقاءه عليه. لكن جيلمور لم يكتف بأن يعلم القاضي بأن الحقوق التي نصّ عليها الدستور (التعديل الأول) قد انتهكت، بل أعلم مراسلي الصحف المحليين بالقصة أيضاً.

بعد ذلك بيومين تراجعت الحكومة، ورفعت الحظر المفروض على النصين رسمياً. لكن جيلمور استمر في السؤال عن الكتب الأخرى، وطلب أن يعلن القاضي أن قانون التجسّس يمثّل قمعاً لحرية التعبير منافٍ للدستور. وعندما سأله أحد المراسلين إن لم يكن في موقفه إضعافاً للأمن القومي، لم يبد أسفاً وقال: «إننا لا نسعى إلى تهديد الأمن القومي، بل لنبذ فكرة بيروقراطية عن الأَمن القومي، ترجع إلىٰ زمن الحرب الباردة وعفا عليها الزمن. إنهم [الحكومة] ينتهكون حرية وسرية المواطنين. وذلك لحمايتنا من غول لن يقوموا بوصفه لنا». .

بدأ هيوز وماي بالعمل مع جيلمور (لم يوافق هويتفيلد ديفي إلاّ لاحقاً، على الاشتراك بصفة استشارية) في التخطيط للقاء حقيقي للحركة المقترحة.

كان هيوز في ذلك الوقت يطلق على المجموعة اسم هواة الكريبتوجرافيا للامسؤولية الاجتماعية [واختصاراً] CASI كاسي. أمضى هيوز وماي الصيف كله، في التحضير وإرسال الدعوات للحدث العالمي في 19 أيلول/ سبتمبر 1992 في منزل هيوز في بيركلي. وقرّروا أن يكون شعارهم التكتم، ذلك أن طبيعة المغامرة، كانت تتضمن هجوماً ضمنياً، على أكثر وكالات الجاسوسيَّة التابعة للحكومة قوة.

تجاوز اللقاء توقعات الجميع، وعلى العكس من أكاديميي بيركنستوكد والأشباح الفضوليين الذين التقوا في مؤتمرات الكريبتو. فإن الحضور الذين بلغ عددهم حوالي العشرين كانوا أشخاصاً ينظرون إِلىٰ الكريبتوجرافيا على أنَّها خارج نطاق عملهم تماماً (إذا كان لديهم عمل، ذلك أن بعضهم كان بلا عمل). وكان همّهم الأساسي هو كيف سيستخدم الناس أدوات التشفير، وكيف يجب استخدامها. كانت سياساتهم شديدة المناصرة لمذهب الحرية. وكان الكثير منهم يعلنون الانتماء إِلىٰ جماعات متطرفة، وكانت فلسفتهم تمزج بين نظرة متطرفة إِلىٰ الحريات الشخصية واعتقاد خيالي. إن الحدود البعيدة للبحث العلمي سوف تكون في وقت قريب لصالحنا. (وقد تضمنت الموضوعات التي أدارت رؤوس المتطرفين تكنولوجيا الجزيئات الدقيقة، والتحكّم الآلي وفيزياء الحرارة المنخفضة؛ وكان بعض هؤلاء المتطرفين قد تطوّعوا ليتم تجميد رؤوسهم بعد وفاتهم، وذلك ليصار إِلىٰ تذويب الجليد عنها، ويعودوا إِلىٰ الحياة في قرن من القرون لا بدّ قادم).

لكن من الخطأ أن نسيء الحكم على الجماعة لهفواتهم أَو للنتائج المتواضعة التي انتهى إليها هذا اللقاء الأول. في الواقع، انتهى الأمر فيما بعد بأن أصبحوا على قدر عظيم من النفوذ لدرجة أن أكثر خيالاتهم تطرفاً باتت موضع دفاع المدافعين. مجدفين وغريبي الأطوار ومتناغمين تماماً مع أنغام الرقصات الرقمية لإيقاع الإنترنيت، لقد كانوا كريبتوجرافيين، وأصحاب

موقف. وإذا لم يكن لدى الحكومة من الأمور التي تشغلها في مجالات الصناعة والمدافعين عن السرِّيَّة، والإصلاحيين والمطالبين بحرية التشفير، كان ظهور ثوار الشّيفرة ليصبحوا أبطال الثقافة الشعبية هي النقطة التي فاضت بها الكأس، وهي إشارة غير متوقعة إِلىٰ أن حروب الشيفرة، قد انتقلت إِلىٰ موقع جديد. ها قد أتى ثوار الشّيفرة، ملوحين بسلاح فكري قوي: فوضى التشفير.

قدَّم تيم ماي، نشرة من سبعة وخمسين صفحة، أعدها خصيصاً لهذا اللقاء الأول، بالإِضافة إِلىٰ جدول أعمال موسّع يتضمن نقاشاً لـ «المضامين الاجتماعية للكريبتوجرافيا»، و«شبكات التصويت»، و«أسواق المعلومات المجهولة». وكانت هناك تقارير عن الأموال الرقمية في فرضيات واقعية، وتقييم جون جيلمور لوكالة الأَمن القومي. وكان هناك بعض الوقت تم ادخاره، بالطبع، «لقرّاء البيانات الرسمية». وكان تيم قد أعد بياناً خصيصاً لهذا اللقاء، أطلق عليه «بيان فوضوي التشفير». انتهى بملاحظة محفزة.

مثلما غيرت تكنولوجيا الطباعة، وقلَّصت نفوذ نقابات الحرف في العصور الوسطى، وبنية السلطة الاجتماعية، كذلك فإن الطرائق الكريبتوجرافية الأساسية ستحدث تغييراً جذرياً في طبيعة الشركات الكبرى وتدخل الدولة في العمليات الاقتصادية. إن فوضى التشفير مجتمعة مع أسواق المعلومات الصاعدة، سوف يُخلق سوقاً سائلة لكل المواد التي يمكن وضعها في كلمات وصور. فكما أن اختراعاً ثانوياً في ظاهره مثل الأسلاك الشائكة قد جعل من الممكن تسوير وفصل المزارع الكبيرة، وبذلك أحدث تغييراً في مفاهيم الأرض وحقوق الملكية في الغرب الجديد، كذلك فإن الاكتشاف الهامشي ظاهرياً الذي حدث في فرع سري من فروع الرياضيات أصبح بمثابة «مقراض السلك»، الذي فك الأسلاك الشائكة حول الملكيَّة الفكريَّة.

انهض، أيها العالم؛ فليس لديك ما تفقده سوى أسوارك من الأسلاك الشائكة.

دعي الناس للاشتراك في «لعبة فوضى التشفير»، لمدة ساعتين، وهو تمرين تقمص أدواراً يتخيّلون فيه، استخدامهم بروتوكولات تشفير غريبة جداً لتعمية أنظار المراقبين لنشاطاتهم، مثل تحرير الأسرار أو عقد صفقات مخدرات. ولما كان برنامج بي جي بي 2.0 قد صدر قبل أيام قليلة من انعقاد المؤتمر ـ ومعظم الحاضرين كانوا معجبين أشد الإعجاب بنسخته الأولى ـ فمضى معظم اللقاء في مناقشة آخر جهد قدمه فيل زيمرمان، ووزعت نسخ من البرنامج لجميع المتواجدين في الغرفة. (كان زيمرمان نفسه لا يزال في بولدر). وتحول الحدث إِلىٰ عمليَّة تبادل مفاتيح، حيث تبادل الجميع مفاتيح بي جي بي العامة ووقَّعوا حلقة مفاتيح بعضهم البعض. فبعد كل شيء، كان برنامج بي جي بي تجسيداً لإيمان المجموعة بأن الكريبتوجرافيا أهم من أن تترك للحكومة، أَو حتَّى للشركات ذات النوايا الحسنة. وحدهم الأفراد المخلصون، المستعدون لتحمّل النتائج المترتبة على العقوبات التي تفرضها الحكومة، هم الذين يستطيعون أن يضمنوا، تداول الأدوات عبر الدورة الدموية للإنترنيت. وفيما بعد، قال جون جيلمور: «إن قمع هذه التكنولوجيا يتطلّب وجود دولة أمنية قوية جداً».

ومن الأحداث الهامّة غير المتوقعة في المؤتمر ملاحظة أوردتها رفيقة هيوز، وهي كاتبة ترتدي الجلد، وتنشر كتاباتها في المجلة الهبية الرقمية «موندو 2000»، تحت اسم سانت جود. فبعد أن استمعت إِلىٰ رؤى مجتمع متقلّب ذي رياضيات متكاملة، وجدت الرابطة التي تجمعهم بمن صعدوا مؤخراً وأطلق عليهم اسم «زعران الكومبيوتر»، متسلّلون إِلىٰ الكومبيوتر تحولوا إِلىٰ علماء بربطهم تحطيم المقدسات جهاراً الذي عرف به متمردون من أصحاب موسيقى الروك بالثورة الرقمية. صرخت المرأة يومئذ: «اسمعوا، إنكم زعران الشّيفرة!» ولقد هاموا جميعاً بهذا اللقب.

كانت المجموعة الملقبة حديثاً توّاقة لتجتمع ثانية خلال شهر من الزمن.

وفي تلك الأثناء، أعد إريك هيوز مكاناً للقاء، زعران الشّيفرة أكثر نشاطاً وخصباً: الإنترنيت. مستخدماً مخدم الشبكة لدى جون جيلمور، (كان اسم مجاله ضمن الشبكة Toad.com) كمحور العالم التخيلي، وأنشأ هيوز ما يُعرف بقائمة التخديم، وهو نقاش مستمر يجمع بين الملايين حيث يتلقى أي شخص سجل اسمه في قائمة البريد الإلكتروني الكامل مساهمات أي عضو آخر يهتم بتقديم أخبار أو نقد نظام تشفير، أو إطلاق العنان لحديث صاخب. وفي غضون أسابيع قليلة، سجل أكثر من 100 شخص أسماءهم على القائمة، وهو عدد مثير بالنظر إلىٰ الحجم الهائل للرسائل المحررة والتي قد تصل إلىٰ أكثر من 150 رسالة في اليوم.

بعد ذلك اللقاء الأول، كتب أريك هيوز مسودة أطلق عليها اسم «إعلان نوايا قصير» وذلك لشرح ما ترمي إليه المجموعة. لقد تصور البيان الرسمي لزعران الشيفرة هذا، بنية سرية تم طبخها في البيت ولا يمكن للحكومة أن تفككها:

يكتب زعران الشّيفرة رمزاً. إنَّهم يعلمون أن على أحدهم أن يكتب دفاعاً عن السرِّيَّة، ولما كانت المسألة هي سريتهم، فسيكتبونها. ينشر زعران الشّيفرة رمزهم ليتمكن رفاقهم من زعران الشّيفرة من التعامل معه وتشغيله. يدرك زعران الشّيفرة أن السرِّيَّة لا يمكن بناؤها في يوم واحد وهم صبورون مع التطور المتزايد.

إن زعران الشّيفرة لا يبالون إذا كنت لا تحب البرمجيات التي يكتبونها. إن زعران الشّيفرة يعلمون أن البرمجيات لا يمكن تدميرها. زعران الشّيفرة يعلمون أن نظاماً منتشراً على نطاق واسع، لا يمكن إيقافه.

إن زعران الشّيفرة، سيجعلون الشبكات آمنة للسرِّيَّة.

بعد ذلك بيومين، أعلن هيوز تفاصيل اللقاء الثاني، والذي سيقام في 10 تشرين الأول/ أكتوبر في المقر الجديد لشركة سانيوز في ماونتين فيو. وقد

كتب في هذا قائلاً: «إن الحضور ثقة مختلفة الأعماق. ادعوا من تشاؤون. . . لكن لا تنشروا الإعلان. فسيحين وقت ذلك».

وهذا ما كان فعلاً. فبحلول العام التالي اتسعت القائمة لتشمل أكثر من 700 مشترك. وقد تلاشت مقاومة المجموعة في الأساس لمنع الصحفيين من حضور لقاءاتهم، وهو موقف مثير للسخرية من أشخاص متحمسين جداً لنشر المعلومات في عصر الإنترنيت. وسرعان ما أصبحت أخبار المعارف المكتسبة لزعران الشّيفرة مادة رئيسة في مطبوعات تتراوح من مجلة وايرد إلىٰ نيويورك تايمز. (وجوههم تختبئ وراء أقنعة عليها خربشات من بصمات المفتاح العام لبرنامج بي جي بي، كانت تزين العدد الثاني من مجلة وايرد). لقد أصبح لوجه الشّيفرة مسحة علمية مستحدثة.

كانت فوضى التشفير مفهوماً ساحراً، لم تقتصر عدواه على وسائل الإعلام فحسب، بل انتشرت لتشمل أوساط الشركات الضخمة الحسنة التنظيم والحكومة كذلك. حتّى دون باركر، وهو خبير أمني معروف وكانت له خبرة قديمة، لتخصصه في تقييم متلصصي الكومبيوتر، أخذ الآن يفكر ملياً في الأخطار الناجمة عن «حالة فوضى المعلومات القادمة إذا ما سمح للشيفرة أن تنتشر دون ضابط وهي على حالتها الراهنة». (أوصى باركر بشيفرة قوية، شرط أن تكون المفاتيح الأصلية في أيدي الحكومة ـ وقد اتضح أن الحكومة كانت تنظر في هذا الأمر).

لكن مع أن ثوار الشّيفرة، أصبحوا الأثيرين لدى الإعلام، وخطراً يتهدد الحكومة، وأبطال الحريات المدنية، إلاّ أن قلة كانت تدرك أن الأساس الرياضي والفلسفي لجهودهم قد تأتى من رجل واحد، يجادل فيه البعض بأنه قمة زعران الشّيفرة. لم يحضر لقاء على الإطلاق، ولم يسجل اسمه في القائمة، وفي الواقع كانت له خصومة شديدة مع بعض أفراد المجموعة. وبالرغم من ذلك، فإن أفكاره وبراءات الاختراع التي كان يحتفظ بحقه فيها عند

تطبيقها، كانت تناقش برهبة وخوف، في عالم الشركات الكبيرة والاستخبارات. كان المبتكر نفسه، واحداً من أكثر الألغاز المحيرة في هذا الحقل، وحله أصعب من حل معيار تشفير البيانات الثلاثي. كان هذا الرجل ديڤيد تشوم.

كان تشوم رجل ذو لحية وشعر طويل، يربطه بشكل ذيل حصان، وهو كريبتوجرافي من بيركنستوكد ورجل أعمال. وقد تخرّج من جامعة بيركلي، وبمبادرة منه، استمرت مؤتمرات الكريبتو، في البقاء، كما نظم الجمعية الدولية لأبحاث علم الشّيفرة. لكن إرثه في عالم الشّيفرة امتد بعيداً، وتجاوز هذه الحدود: فلعدد من السنين كان دون كيشوت ثورة السرِّيَّة، ويسعى بمثالية إِلىٰ تحرير الشّيفرة من قبضة الأخ الكبير. ومنذ أن كان على مقاعد الدراسة في جامعة بيركلي في واخر السبعينات، أخذ في البناء على أساس المفتاح العام، من أجل ابتكار بروتوكولات لعالم يمكن للناس فيه القيام بما يشاؤون من العمليات الإِلكترونية وهم محافظون على هويتهم مغفلة من الاسم. وإذا كان استخدام المفتاح العام شبيهاً بالسحر، وإذا كانت التطويرات مثل تبادل الأسرار وبراهين المعرفة الصفرية تعتبر أمثلة قوية على هذا السحر، فإن ديڤيد تشوم كان بمثابة الساحر «هوديني» بالنسبة للشيفرة، فقد اخترع أدوات في الرياضيات يمكنها أن تأتي بالمستحيل: منافع العالم الإِلكتروني كلها من دون مثالب الطريق الإِلكترونية التي يمكن أن ترشد المحتالين، والشركات الكبرى، وعناصر الشرطة إِلىٰ عتبة بيتك. إن ذلك السحر يملك إمكانية، كما يعتقد البعض، أن يجعل مفهوم الدولة برمته يختفي.

أبدى ديڤيد تشوم، منذ نعومة أظفاره، اهتماماً بالعتاد المتصل بالسرِّيَّة. ويقول: «أعتقد أن من المهم إدراك، أن هناك قوة تدفعني بشدة. ولقد جاء اهتمامي بأمن الكومبيوتر أساساً، والتشفير لاحقاً، من افتتاني بتقنيات الأمان عموماً ـ أشياء مثل الأقفال وأجراس الإنذار والخزائن الفولاذية». (وفي فترة ما،

عندما كان طالباً في الدراسات العليا، ابتكر تصميماً جديداً لقفل، وكاد أن يبيعه لمصنع كبير). وكان، بالطبع، مفتوناً بالكومبيوتر. نشأ تشوم وترعرع في إحدى ضواحي لوس أنجليس، في عائلة يهودية من الطبقة الوسطى (لم يتحدد تاريخ ميلاده بسبب ما هو معروف عنه، من ميل لعدم إفشاء مثل هذه التفاصيل المحددة للهوية). واشتغل منذ أن كان على مقاعد الدراسة الثانوية فالجامعية، بدأ بحضور المحاضرات في جامعة كاليفورنيا بلوس أنجليس قبل أن ينال الشهادة الثانوية، ثم التحق بجامعة سونوما الحكومية ليكون قريباً من صديقته، وانتهى بنيل الشهادة الجامعية من جامعة كاليفورنيا بسان دييجو ـ بأعمال الكومبيوتر المتنوعة المألوفة على سبيل التسلية: مثل اكتشاف كلمة السر، والبحث في سلة المهملات وما شابه ذلك. وفي دروس الرياضيات كان يصاحب أمثاله من الرفاق الساخطين: إذ كانوا يجلسون في المقاعد الخلفية، ويدأبون على الرد على الأستاذ حينما يأتي بخطأ، فيأتون ببرهان مناقض لقوله. (لم يكونوا مشاغبين بالمعنى الدقيق للكلمة، لكنهم كانوا يتحلون بالجرأة في مجال الكومبيوتر). كذلك تحقق له أن ينال معرفة أساسية جيدة بالرياضيات. ثم في وقت متأخِّر من حياته الجامعية، وقّع على موضوع الكريبتوجرافيا، وإذا نظر المرء إلىٰ تلك المقدمات يرى أن هذا التطور في حياته كان من طبيعة الأمور.

لطالما كان يفكّر في أمر الوسائل التي توفر الحماية للمعلومات الموجودة في الكومبيوتر، لكنَّه أظهر أفكاره الجادة الأولى في هذا الموضوع في حلقة بحث قدَّمها في مادة اللغة الإنكليزية. فالمدرسة الشابَّة ذات الاتجاهات الراديكالية في السياسة التي تدرس هذه المادة كانت قد حثَّت الطلاَّب على الكتابة عن أمور تثير اهتمامهم فكتب تشوم عن التشفير.

اختار تشوم جامعة بيركلي للتحضير للدراسات العليا، وذلك بسبب ارتباطها بالنموذج الجديد لكريبتوجرافيا المفتاح العام. كان يعلم أن لانس هوفمان، الذي كان يدرس هناك، هو أستاذ رالف ميركل. لكنَّه لم يكن يدري أن

هوفمان قد رفض النظر في آراء ميركل. ومع ذلك، فقد عقد صلات جيدة في الجامعة ـ حتّى أنه التقى هويت ديفي الذي كان يعيش في بيركلي آنذاك ـ وحصل على الدعم الذي يحتاج إليه ليبدأ عمله الخاص. وإن أوراق تشوم الأولى، التي طبعت عام 1979، تفصح عن المنحى الذي ستتخذه أعماله: ابتكار وسائل كريبتوجرافية لضمان السرِّيَّة. وكانت أفكاره مبنية على مفهوم المفتاح العام، وبشكل خاص على ميزات التحقّق من التوقيع الرقمي. ويقول: «لقد أصبحت مهتماً بهذه التقنيات على وجه الخصوص لأنني أردت عمل بروتوكولات تصويت مغفلة الاسم. ثم أدركت أن بإمكان المرء استخدامها بشكل أكثر عمومية كنوع من بروتوكولات الاتِّصالات التي لا يمكن تعقبها». وإن سلوك هذا الدرب يؤدي، إلىٰ نقود رقمية مجهولة المصدر ولا يمكن تعقبها.

يرى تشوم أن السياسة والتكنولوجيا تعززان بعضهما البعض. أما بالنسبة للسرِّيَّة، فكان يعتقد أن المجتمع يقف على مفترق طرق. وأن المضي في الاتجاه الذي نسير فيه حالياً، سوف يحملنا إلىٰ حيث تحققت أسوأ نبوءات أورويل. وقد صور المشكلة بدقة في بحث بعنوان «الأرقام، يمكن أن تكون شكلاً للنقد أفضل من الورق»:

إننا نقترب بسرعة من لحظة اتخاذ قرار حاسم، وربما لا يمكن الرجوع عنه، وهو يتصل بالاختيار لا بين نوعين من الأَنظمة التكنولوجية، بل بين نوعين من المجتمع. فالتطورات الجارية حالياً في تطبيق التكنولوجيا جعلت ما تبقى من ضمانات للسرِّيَّة والحق في الوصول إلىٰ البيانات الشخصية وتصحيحها مسألة جوفاء بلا معنى. وإذا استمرت هذه التطورات فإن إمكانياتها العظيمة في الرقابة ستجعل حياة الأفراد مكشوفة للرصد، وضعيفة أمام السلطة على نحو لا سابق له.

في أوائل الثمانينات، أجرى ديفيد تشوم بحثاً لإيجاد حل لمشكلة، بدا أن من المستحيل حلها، لأن الكثير من الناس لا يعتبرونها مشكلة بالمقام

الأول: كيف يمكن لميدان الحياة الإلكترونية أن يتوسّع دون تهديد سريتنا؟ أَو بعبارة أكثر جرأة، هل بإمكاننا القيام بذلك عن طريق زيادة السرِّيَّة فعلياً؟ وفي غضون ذلك اكتشف كيف يمكن للكريبتوجرافيا أن تنتج نسخة إلكترونية من ورقة الدولار.

من أجل تقدير ذلك على نحو كامل، على المرء أن يفكر في المعوقات أمام مهمة كهذه. فالأمر المقلق على نحو مباشر لأي شخص يحاول إنتاج شكل رقمي للعملة هو تزوير العملة. كما أن أي شخص قام بنسخ برنامج من قرص مرن إلىٰ سواقة صلبة يعلم أنه أمر بمنتهى البساطة إنتاج نسخة مطابقة تماماً لأي شيء في الحقل الرقمي. فما الذي يمنع إيف من أخذ دولارها الرقمي الوحيد وإنتاج مليون أو بليون نسخة عنه؟ إذا كان بإمكانها القيام بذلك فإن كومبيوترها النقال، وكل كومبيوتر، أخر يصبح آلة لصك العملة، وإن تضخماً مفرطاً يجعل مثل هذا النوع من العملة لا قيمة له.

كانت طريقة تشوم في التغلّب على المشكلة هي استخدام تواقيع رقمية لتأكيد صحة الأوراق النقدية. يتم تحديد رقم متسلسل وحيد لـ «ورقة نقدية» معينة ـ ويصبح الرقم نفسه هو الورقة النقدية ـ وعندما يتم تقديم هذا الرقم الفريد إلىٰ تاجر أو مصرف، فبالإمكان فحصه بدقة لمعرفة إذا كانت الورقة الفعلية أصلية ولم تصرف من قبل. سيكون القيام بذلك سهلاً إذا تم تعقّب كل وحدة إلكترونية للنقد عبر النِّظام في كل نقطة، لكن هذه العمليَّة يمكن لها أن تتعقب الطريق التي يصرف الناس فيها أموالهم، حتَّى آخر قرش منها. وهو بالضبط ذلك النوع من كابوس المراقبة، الذي يخيف تشوم. فكيف يمكنك القيام بذلك وفي نفس الوقت تحمي إغفال ذكر اسم المرء بشكل مطلق.

بدأ تشوم حله، عن طريق الإتيان بشيء يدعى «التوقيع الأعمى». وهي عملية يمكن للمصرف من خلالها، أَو أي وكالة مخولة، إثبات أصالة رقم بحيث يمكن له أن يقوم بعمل وحدة نقدية. مع ذلك فباستخدام عمليات تشوم

الرياضية، فإن المصرف ذاته لا يعلم من لديه الورقة النقدية، ولذلك لا يستطيع تعقبها. وبهذه الطريقة، عندما يعطيك المصرف سيلاً من الأرقام التي صُمّمت لأن تقبل على أنّها نقد، فإن لديك طريقة لتغيير الأَرقام (لتضمن أن الأموال لا يمكن تعقبها) وفي الوقت ذاته تحافظ على موافقة المصرف.

كان أحد أكثر كشوفات تشوم أهمية قد حصل، عندما استطاع أن يبرهن رياضياً، على أن هذا النوع من إغفال الاسم، يمكن توفيره على نحو غير مشروط. وجاءت لحظة الإلهام عندما كان يقود سيارته الفولكسفاكن الفان من بيركلي إلىٰ بيته في سانتا بربارة، حيث كان يدرِّس علوم الكومبيوتر في أوائل الثمانينات. ويصف ذلك بقوله: «كنت أقلب هذه الفكرة مرّات ومرّات في رأسي، ودرست الحلول كلها بعناية. ثم أمعنت التفكير في الأمر، وأخيراً في الوقت الذي توصلت فيه إلىٰ الحل، عرفت تماماً طريقة القيام به على أحسن وجه».

وقد قدم نظريته مع مثال حي: سيناريو عن ثلاثة كريبتوجرافيين، انتهوا من تناول طعام العشاء في مطعم وينتظرون الفاتورة. يظهر النادل ويقول لهم، أن الفاتورة دُفعت مسبقاً. والسؤال هو، من الذي دفع الحساب؟ هل قرَّر أحد الحاضرين أن يدعو زملاءه دون إعلامهم بذلك ـ أم أن وكالة الأَمن القومي أَو شخص آخر قام بدفع ثمن وجبة العشاء والمعضلة هنا ما إذا كان بالإِمكان الحصول على هذه المعلومات دون كشف هوية الكريبتوجرافي، الذي يحتمل أنَّه دفع ثمن العشاء.

إن حل مشكلة «عشاء الكريبتوجرافيين» كان بسيطاً على نحو يدعو للدهشة، فهو يتضمن رمي قطعة نقد مخفية عن أنظار أشخاص معينين عدة رميات. فعلى سبيل المثال، يمكن لكل من أليس وبوب، أن يقوما برمي قطعة النقد عدة مرات خلف قائمة الطعام بحيث لا يستطيع تيد رؤيتها، ثم يقوم كل منهما بكتابة النتيجة على انفراد وتقديمها له. والشرط الأساسي أنَّه في حال كان أحدهما، هو المضيف الكريم الذي دفع ثمن العشاء، فإن ذلك الشخص

سيكتب النتيجة المعاكسة لرمي قطعة النقد. وهكذا إذا تلقى تيد تقريرين متضاربين لرمي قطعة النقد ـ واحدة طغراء، وأخرى نقش ـ فإنه سيعلم أن أحد الذين تناولوا العشاء قد دفع الحساب. ولكن بدون تواطؤ آخر ليس لديه طريقة لمعرفة أيهما الذي دفع، أليس أم بوب. وعن طريق سلسلة من رميات النقد وتمرير الرسائل، فإن أي عدد من متناولي العشاء ـ في ما يدعى شبكة عشاء الكريبتوجرافيين DC-Net ـ بإمكانهم أداء هذه اللعبة. ويمكن للفكرة أن تكون مقياساً لنظام النقد. ويقول تشوم: «إن هذه الفكرة هامة جداً، لأنّها تعني أن استحالة التعقب يمكن أن تصبح حالة مطلقة. ولا يهم ما لدى وكالة الأَمن القومي من كومبيوترات قوية لفك الرموز ـ فلن يستطيعوا اكتشافها، وبإمكانك إثبات ذلك». وهو يعني أنّها رياضياً بمثابة واق من الرصاص.

إن أعمال تشوم اللاحقة، وكذلك براءات الاختراع التي تقدم بها بنجاح، قد تأسّست على تلك الأفكار، وتعالج مشكلات مثل الحيلولة دون الإنفاق المزدوج مع الحفاظ على إغفال اسم المنفق. وبخدعة رياضية ذكية بشكل خاص، توصل إلىٰ خطة يمكن من خلالها المحافظة دوماً على إغفال الاسم، باستثناء حالة واحدة: إذا أقدم الشخص على عملية إنفاق مزدوج، لوحدة نقدية كان قد سبق له أن أنفقها في مكان آخر، عندئذ يسمح الجزء الثاني من المعلومة بالتعقب، والاستدلال على المصدر. وبتعبير آخر، فإن الغشاشين وحدهم يمكن تحديد هويتهم بالفعل. وبعملهم هذا يكونوا قد قدَّموا دليلاً، لقوى حفظ النِّظام على محاولتهم الاحتيال.

كان ذلك عملاً مثيراً، لكن تشوم لم ينل من التشجيع على المثابرة إلاّ القليل. وفي هذا يقول: «كان من الصعب جداً بالنسبة لي أن أعمل في موضوعات كهذه في هذا الحقل لسنوات كثيرة، لأن الناس لم يكونوا يتقبّلون الأمر على الإطلاق». ففي أوائل الثمانينات وعلى مدى سنين كثيرة، حاول تشوم عقد صلات شخصية مع الشخصيات الهامّة والمشاعل الهادية التي تحدِّد سياسة السرِّيَّة وبسط لهم أفكاره.

يقول تشوم: «كان رد الفعل الرسمي سلبياً، ولم أتمكّن من فهم السبب. وهذا جعل من الصعب علي الاستمرار في متابعة العمل، ذلك أن المستشارين الأكاديميين الذين كنت أرجع إليهم في البحث، كانوا يقولون، «إن هذا موضوع سياسي، وذلك اجتماعي، لقد تجاوزت الحد»». حتّى مستشاره في جامعة بيركلي حاول أن يثنيه عن متابعة البحث، قائلاً لتلميذه العنيد: «دعك من هذا الموضوع، إنك لا تستطيع أبداً أن تتنبأ بتأثير فكرة جديدة على المجتمع». وعوضاً عن الإصغاء للتحذير، قام تشوم بإهداء أطروحته لذلك المستشار، قائلاً: إن رفضه لتفكير مستشاره هو ما حثّه على إنهاء العمل.

وأخيراً، قرَّر تشوم، أن أفضل طريقة لنشر أفكاره هي إنشاء شركته الخاصة. وفي ذلك الوقت كان يعيش في أمستردام؛ ففي زيارة سابقة لهذه المدينة مع صديقته الهولندية، التقى مصادفة ببعض الأكاديميين، وعُرض له أن يشغل منصباً، وهذا قاده لأن يصبح موظفاً، في مركز الرياضيات وعلوم الكومبيوتر في أمستردام CWI. وهكذا أسَّس في عام 1990 شركة ديجيكاش، برأسماله القليل وعقد جاهز في يده من الحكومة الهولندية لدراسة الجدوى الاقتصادية لتقنية تتيح دفع رسوم الطرقات العامة إِلكترونياً. طور تشوم نموذجاً أولياً حيث يثبت على زجاج السيارة بطاقات ذكية تحمل ما يعادل مبلغاً معيناً من المال وتقوم أجهزة فحص سريعة جداً باقتطاع الرسوم فيما السيارات تمر مسرعة بجانبها. كذلك يمكن للمرء استخدام البطاقات لدفع تكاليف استخدام وسائط النقل العام، وأخيراً لأشياء أخرى. وبالطبع فإن الدفع يتم وتبقى هوية الدافعين مغفلة. فبالنسبة لتشوم كان هذا أكثر الأجزاء أهمية في النظام: وخوفه هو أن خطة تتيح للمسؤولين تعقب المواطنين على الطرقات ستكون واحدة من الأهوال التي عرض لها أورويل. (الأنظمة التي طبقت أخيراً في الولايات المتّحدة، مثل نظام E-Z Pass الشهير تقوم فعلاً بتعقب المسافرين).

بعد إنهاء ذلك العقد (لم يطبق النظام أبداً)، استمر تشوم في تشغيل

شركته في تطبيقات البطاقة الذكية؛ وركزت بعض المشاريع على أَنظمة نقد يمكن استخدامها في عمارة أَو مجمع من الأبنية. وكان لديه مثال عملي في المقر الرئيسي لديجيكاش في أطراف أمستردام؛ يمكن للزوار أخذ عينة عن المستقبل، عن طريق استخدام بطاقات نقد مغفلة الاسم، لشراء الصودا وإجراء المكالمات الهاتفية.

لكن في أوائل التسعينات، وحتَّى مع إدراك العالم لأهمية أفكار تشوم التي أنتجها في العزلة. إذ أن شركات مثل مايكروسوفت وسيتي بنك كانت تسعى وراء مشاريع النقد الرقمي، فإن نطاق عمليات الشركة [ديجيكاش] كان ما يزال ضيقاً نسبياً. وظلت ديجيكاش مستقلة، ولم تدخل في تحالف وثيق مع شريك كبير، في مجال المصارف أَو الخدمات المالية. شعر تشوم أن هؤلاء الشركاء، أَو على الأقل من سيحصلون على رخصة استخدام تقنية ديجيكاش سيظهرون مع مرور الزمن. وأنَّهم لا بد أن يظهروا. وقد أصبح الرأي المتفق مع الحكمة الآن، أن الأرقام المحمية بالشيفرة سوف تحل محل الأَوراق النقدية. وعندما يحصل ذلك. فإن الصيغ الرياضية التي ابتكرها ستصبح عاملاً حاسماً في الحفاظ على السرِّيَّة، في عصر الأموال الإِلكترونية. كانت هذه هي الفكرة التي اعتقد تشوم أنَّها جديرة بالمتابعة والتمسّك بها.

رأى البعض في هذا الموقف عناداً ومكابرة، أَو على الأقل، ضعف في الخبرة التجارية. ويقول موظف سابق في ديجيكاش: «أراد الناس شراء براءات اختراع ديفيد لكنَّه كان يبالغ في ما يطلبه». وهناك قصة أخرى شائعة هي أن تشوم قرَّر في آخر لحظة رفض صفقة مع شركة فيزا والتي كانت ستجعل ديجيكاش معياراً للأموال الإِلكترونية. وقد أخبر مدير تنفيذي في ديجيكاش أحد المراسلين عن حالات فشل مشاريع عقود مع شركات أخرى، بما فيها مايكروسوفت. لكن تشوم قاوم بشدة نظرية أن شذوذ طباعه وتصرفاته أعاقت عقد صفقات هامة. وعندما أجرى أحد المراسلين، مقابلة معه حول هذا

الموضوع، اندفع تشوم يرد بعنف: «إنه افتراء خبيث القول أن من الصعب عقد اتفاقات معي». ومع ذلك، فقد بدأت بعض الشركات ـ التي شعرت بالإحباط لعدم قدرتها على الحصول على براءات اختراع تشوم ـ بابتكار مشاريعها الخاصة فيما يتعلّق بإبقاء الاسم مغفلاً، والتي قد تكون انتهكت، أَو لعلها لم تنتهك براءات اختراعه.

شعر بعض زعران الشّيفرة أن تشوم، اتّخذ توجهاً غير لائق أيديولوجياً بتقدّمه لطلب براءات اختراع لأعماله. (كذلك كان هؤلاء المثاليين غير معجبين ببراءات اختراع آر إس إيه، أيضاً). وكانوا يشتكون أنّه بحجبه التكنولوجيا عن أي شخص يريد تطبيقها ـ وتهديده بمقاضاة أي شخص اختبر آفاق براءات الاختراع هذه ـ كان في الواقع يحول دون تحقيق أحلامه. وأثار هذا النقد غضب تشوم، وردّ بالقول: «إني أعتقد بأن أمراً كهذا ربما كان ممكن التحقيق، وشعرت بحق أن القيام به هو مسؤوليتي. وما من أحد كان يعمل على هذا مدة ست سنوات بينما كنت منشغلاً أعمل فيه والجميع يظن بي الجنون. إن براءات الاختراع مفيدة جداً لشركتنا الصغيرة؛ ولم يكن بالإِمكان الحصول على ترخيص للعمل دون براءات الاختراع، ومن وجهة نظري فإن الهدف منها هو إخراج العمل إِلىٰ حيِّز الواقع».

كان زعران الشّيفرة يؤمنون، بأن بروتوكولات إغفال الأسماء سوف تلاقي رواجاً. وأن ذلك نتيجة محتومة. وحاول العديدون القيام بمشاريعهم الخاصّة، مستخدمين أسماء مثل ماجيك موني. وفي نفس الوقت، كان سيتي بنك وفيزا يدرسان النقد الرقمي بمعزل عن الآخرين. وتمّ تأسيس شركة جديدة بدعم مادي جيد خارج واشنطن العاصمة دعيت سايبركاش؛ وكانت شركة آر إس إيه داتا سيكيوريتي أحد المستثمرين فيها. وأراد زعران الشّيفرة معرفة ما إذا كان هذا الشكل الجديد من المال سوف يسمح بتعقّب المستخدم إِلكترونياً. وكانوا يأملون بألاّ يكون الأمر كذلك. كانت لائحتهم مليئة بالسيناريوهات ومنها أن

الإنترنيت توفر «ملاذاً للبيانات» خارج الولايات المتّحدة. في أماكن خارج نطاق سلطة الدول الصناعية الكبرى حيث بإمكان الناس إيداع أموالهم في البنوك، أَو حتّى المقامرة باستخدام النقد الرقمي. وعندما ساعد بعض زعران الشّيفرة في تنظيم أول مؤتمر حول الكريبتوجرافيا المالية كان اختيارهم لمكان انعقاده في إنجويلا أمراً حتمياً. ذلك أنّها جزيرة صغيرة في الكاريبي قوانينها التجارية، أقل ما يقال فيها، أنّها حرّة.

كانت إحدى أفكار تشوم التي تبنّاها زعران الشّيفرة بإخلاص، ظهور خدمات تدعى «مدورو الرسائل». وهي نوع من منظفي المعلومات... مواقع أمامية على طريق المعلومات السريعة، يحافظ عليها بشكل مستقل ناشطون من زعران الشّيفرة، ينتزعون أي إشارة مميزة عن الرسالة، ويرسلونها إما إلىٰ وجهتها الأخيرة، أَو إلىٰ مدور آخر للرسائل، لتخضع لجولة أخرى من تنظيف البيانات. تدخل رسالتك في مدور الرسائل (والذي يُعرف كذلك باسم المخدم المجهول) ومعها عنوان المرسل، وتستمر في طريقها دون العنوان.

إن مجرد إرسال رسالتك مغفلة الاسم إلىٰ مدور واحد للرسائل، على الرغم من اعتباره حماية غير كافية، فإنّها في الواقع تعطي الشخص الذي يسيِّر المخدم سلطة بالغة. وإذا اتضح أنه غير جدير بالثقة، أَو تم التسلل إليه، أَو سلّم مذكرة إحضار، فيكون من السهل جداً على الدخلاء الحصول على عنوان المرسل. كانت تلك نفس المشكلة التي اشتكى منها هويت ديفي أصلاً والمتعلّقة بمديري الشبكة وكلمات السر. واعتقد زعران الشّيفرة أن لديهم الحل للتغلّب على هذه المشكلة: إذا تعاونوا على إنشاء اتحاد حر من مدوري الرسائل حول العالم. وللحصول على حماية فعلية، عليك توجيه رسائلك عبر سلسلة، من مدوري الوسائل. وكل خدمة تدوير للرسائل ستنزع عنوان المرسل؛ وسيكون لدى المخدم الأول وحده العنوان الأصلي. عندئذ على الشرطي أَو الجاسوس الذي يحاول تعقب رسالة ما الحصول على سجلات

عشرة أَو اثني عشر أَو عشرين مدور للرسائل (إذا كانت السجلات ما تزال موجودة، والتي على الأغلب غير موجودة) وذلك ليقتفي الأثر ليصل إِلىٰ المصدر. لذا إذا لم تستطع السلطات الحصول على السجلات من أحد مدوري الرسائل الجريئين في تونجا، فإنَّهم لن يعثروا على السجلات الأصلية أبداً. (إن بعض المستخدمين، الذين لديهم جنون اضطهاد [بارانويا] - أَو على الأرجح زعران شيفرة يعرضون برمجياتهم - قد مروا عبر نحو مئة مدور للرسائل في سلسلتهم؛ ولما لم يكن هناك هذا العدد الكبير من المخدمين المجهولين في العالم، فإن الأمر يقتضي القيام بعدة جولات).

لكي تتأكّد بالفعل من إغفال اسمك وحماية سريته، عليك استخدام برنامج بي جي بي لتشفير الرسالة كلها بالمفتاح العام لمدور الرسالة الأخير في السلسلة وبهذه الطريقة لن يتمكّن من قراءتها أي مدور للرسائل سوى الأخير في السلسلة، وتكون الرسالة في ذلك الوقت قد اختفت أصولها تماماً. أتريد إجراءات وقائية أكثر إحكاماً؟ شفّر تلك الرسالة الأخيرة في مغلف آخر من تشفير بي جي بي ويتم هذا باستخدام المفتاح العام لمدور الرسائل قبل الأخير في السلسلة. وسيؤمن ذلك طبقة مضاعفة من التشفير. وهكذا دواليك، مغلفات ضمن مغلفات أخرى، حتَّى تكفل السرِّيَّة التامة. ففي أي نقطة على طول الطريق، إذا حاول شخص ما قراءة الرسالة، فلن يحصل إلاَّ على كلام غير مفهوم. وقد وصف إيريك هيوز ذلك بسرور: «مثل الحصول على شريط من هسيس الميكروفون».

بتشجيع من زعران الشّيفرة، أسَّس هيوز أول مدور للرسائل على مخدم بيركلي، وبحلول عام 1993 كان هناك نحواً من عشرين مدور للرسائل يعملون بنشاط. ومن بين جميع الجهود الحثيثة التي بذلها أفراد القائمة، كان أقواها ابتكار طريق أسهل للإفادة من سلاسل مدوري الرسائل. ويبدو أنَّه لم يزعج زعران الشّيفرة عدم قيام هذا النّظام الناشئ بأي شيء لتحسين المجتمع. فمعظم

الرسائل المرسلة عبر مدوري الرسائل، كانت كتابات موجهة إلىٰ مجموعات النقاش من مستخدمي الشبكة عبر الإنترنيت؛ والأمر المحزن أن هذه الرسائل كانت على العموم مضايقات متلاحقة، لأشخاص أو مجرد ثورات غضب حمقاء. وعوضاً عن إغناء حوارات عالم الكومبيوتر، فإن هذه القنابل النتنة الخالية من التوقيع قد حطّت من هذه الحوارات. قد يكون هناك اتصال بين عدد من الزملاء المثقفين يتحاورون حول مسائل تقنية أو أمور شخصية، ويقوم أحد الحمقى بمقاطعتهم ويلقي إهانات بملء فمه، فيشعر المشاركون الجادون في النقاش بالإحباط، لأنه ما من طريقة لتطبيق عقوبات، على مخرّب الاتّصالات الذي أفسد صفاء الجو. من جهة أخرى، في بعض الجماعات، وبالأخص تلك التي تشجع المساهمات من أصحاب الوجدان الاجتماعي اليقظ، أو ضحايا الجرائم الجنسية. من ناحية أخرى فإن مرسلي الرسائل المعارضين اكتشفوا إجراء للسرّيّة وذلك بترميز رسائلهم بما ينسبها إلىٰ هويات أطراف أخرى لا يمكن اقتفاء أثرها إنما تُعرف بـ «أسماء» ولم يكن بالأمر الغريب في مجموعات كهذه أن ترى الكثير من البريد من مراسلين واضح فيهم التخفي وراء عبارات في مواقع مثل bogus@no.return.address.

إن أصعب جزء في تشغيل مدور الرسائل، كما اتضح، لم يكن تقنياً. فقد يسّرت نصوص زعران الشّيفرة على لمؤهلين تقنياً ولو كانوا غير مختصين بالكريبتوجرافيا عملية إنشاء مخدم مجهول. فالجزء الصعب هو الوقوف في وجه الضغوط الاجتماعية والقانونية والتي ستظهر عندما يطالب المستهدفون من بريد الكراهية ومحبي المزاح بإيقاف المسالك المغفلة الاسم. ومن الحالات النموذجية حالة أزعر الشّيفرة في جامعة واشنطن الذي استخدم نظام كومبيوتر الجامعة مدوراً للرسائل. مضت الأمور على أحسن ما يرام عدة شهور، وكتب المشغل: «لم يكن الأمر سيئاً إذا أخذت بالاعتبار أنه يستند إلىٰ معاناة طالب مع إدارة شبيهة بالحكم النازي. وجاءت الضربة القاضية عندما تقدم إلي أحد المستهدفين، [من هجمات البريد الإلكتروني] يشتكي من أن أحدهم يرسل له

رسائل بغيضة عبر مدور الرسائل الذي أقوم بتشغيله». ووصل طلب إيقاف هذا النوع من البريد إِلىٰ «مدير بريد» النِّظام، الرجل المسؤول عن نظام البريد الإِلكتروني في الجامعة. وبالطبع، لم يكن المدير يعلم شيئاً عن كون خدمة كهذه يتم تشغيلها على كومبيوتر الجامعة، «لقد فوجئ كثيراً حينما درس الأمر!» وتلك كانت نهاية مدور الرسائل.

أما حالة يولف هيلسينجوس فكانت أكثر نجاحاً، وكان هذا فنلندياً خبيراً بالكومبيوتر، بدأ في عام 1993 بتشغيل مدور للرسائل في منزله خارج هلسنكي. إذ أراد التغطية على أشخاص ضمن مجموعة مستخدمي الشبكة (يوسنت جروب)، يتراسلون حول قضايا معالجة الإدمان على الكحول. وقد أنشأ «بينيت» (وهو تحوير لاسم شركته بينيتيك) على جهاز يونيكس يعمل برقاقة متواضعة الإمكانات من نوع إنتل 386. وأطلقه للعمل معتمداً بشكل كلي على مصداقية كلمة المستثمرين. وسرعان ما أصبح آلاف الأشخاص يرسلون عبر الجهاز، الذي يرسلها إِلىٰ وجهتها دون الرأسية التي تحدّد هوية المرسل. ولما أصبحت حركة المراسلة شديدة الكثافة اضطر جلف إِلىٰ أن يركب في منزله أنبوب إنترنيت [للمعالجة التواصلية] ذا سرعة عالية، كانت تكلفته ألف دولار شهرياً. وفي بعض الأحيان، يكتب له بعض المستخدمين يسألونه ما الذي دفعه إِلىٰ هذا العمل. وكان الجواب معقداً: ذلك أن جلف ينتمي إِلىٰ أقلية تتحدّث السويدية في فنلندة وهو يؤيد دعم الأقليات للتعبير عن آرائها. ومن جهة ثانية فإنه يعتبره هواية. ويقول: «ينفق البعض مبالغ مماثلة على الغولف أَو أي شيء آخر». وعندما اشتكى البعض من أنَّه كان يسمح لأشخاص بغيضين ومنحرفين للتعبير عن أنفسهم، رد على ذلك بالتالي:

لا يسعني إِلاَّ أن أجيب باعتقادي الراسخ، بأنَّه ليس لي أن أملي على الآخرين تصرفاتهم. ولكن تذكروا أن الرسائل المغفلة هي امتياز، فلتستخدموها

على هذا الأساس. وأعتقد أن الأشخاص الناضجين يمكنهم التصرّف بمسؤولية. رجائي ألا تخذلوني.

مهما تكن النتيجة فإن جهد زعران الشّيفرة، الذي تمثّل في مدور الرسائل قد ولّد حواراً حيوياً حول قضية إغفال الاسم في المجتمع الرقمي. وكان أحد النصوص الهامة لزعران الشّيفرة لعبة إندر Ender's Game، وهو رواية من الخيال العلمي لأوسون سكوت كارد. وقد تمحور جزء من الحبكة على نقاش عام مؤثر بين اثنين من الفلاسفة المغمورين استغلا تقنية مثل مدور الرسائل، لإرسالها تحت اسمين مستعارين هما ديموستين ولوك. ولما كانت الأفكار هدّامة، كان من الضروري جداً إبقاء هويتهما الحقيقية سراً، وبالرغم من ذلك فإن الحجج التي اعتمداها هذان كانت من القوة بحيث غيَّرت مجرى المجتمع في الرواية. وثمة سبب آخر لإخفاء هوية الأشخاص الحقيقيين الذين وراء هذه الأفكار كون الكاتبين كانا طفلين، صبي وأخته يبلغ عمرهما اثنتي عشرة سنة وعشر سنوات على التوالي. وقال الصبي لأخته شارحاً: «ليس ذنبي إن كان عمري الآن اثنتي عشرة سنة. إن العالم ديمقراطي دوماً في أوقات التغير، وسيفوز الشخص ذو الصوت الأكثر عذوبة».

ولكن لم يكن أدب الخيال العلمي وحده، الذي قدّر إغفال الأسماء حق قدرها. فهذه الممارسة كانت أمراً حاسماً في تشكيل الولايات المتّحدة ذاتها، وكانت على ما يذهب البعض تقليداً أمريكياً مثل فطيرة التفاح. وكما يحب مؤرخو زعران الشّيفرة أن يشيروا إلىٰ أن أنموذج النقاش ربما استلهم النقاش الذي دار في رواية أوراق الفيدرالي The Federal list Papers، ومقتطفات من كتابات جيمس ماديسون، وجون جاي، وألكساندر هاميلتون ولكن نشرت باسم مستعار هو بوبليوس. وعندما كتب توماس بين كتابه Common Sense، كان قد وقّعه أصلاً تحت اسم رجل إنكليزي An English man. وقد أشارت المحكمة العليا «أن الكتيبات والكراسات وحتّى الكتب التي أغفل فيها اسم كتّابها قد

لعبت دوراً هاماً في تطور الإنسانية». وهو دور أيّدته المحكمة في قراراتها. وفي عام 1995، أعادت تأكيد دستورية المفهوم مرة أخرى، مستخدمة عبارات جون ستيوارت ميل في تمجيد إغفال الاسم «درعاً يقي من طغيان الأكثرية». فمن يلوم زعران الشّيفرة لإنتاجهم أدوات كريبتوجرافية، لحفظ قدرة الكاتب على متابعة هذا التقليد الحيوي؟

الكثير من الناس، كما تبيَّن فيما بعد، نقّاد ـ من بينهم مدير مكتب التحقيقات الفيدرالي (إف. بي آي) لويس فريه ـ سيذهبون إلىٰ القول، أنه عندما انتشرت الغفلية Anonymity [إغفال الاسم] عبر الإنترنيت، لم تجد مجرد بيئة ملائمة في وسيط جديد؛ بل تضخم أمرها بما يفوق كل تقدير، وتحوّلت إلىٰ شيء أكثر خطورة. وأدّى اختراع ديڤيد تشوم للتواقيع الرقمية العمياء، والنقد المجهول المصدر والذي لا يمكن تعقّبه، إلىٰ إمكانية جعل الفضاء التخيلي منطقة حرة الهوية حيث بإمكان أحدهم أن يعمل سراً على نحو أسهل بكثير وأكثر فاعلية منه في العالم الحقيقي، وعلى سبيل المثال، عندما تقوم بصرف عملة صعبة في متجر، لا يسألك أحد عن بطاقتك الشخصية، لكن وجهك سوف يسم الصفقة في ذهن أمين الصندوق، وخاصة إذا كنت زبوناً جيداً تتردد باستمرار. (إذا كنت تحمل حقيبة فوق رأسك، فعلى الأرجح أنّك ستجد صعوبة في تسديد الدفعات أساساً). وباستخدام بروتوكولات تشوم بإمكانك القيام بمشترياتك، وإرسال بريدك، وحتّى تلقّي الأموال مع ضمان تام بأنّه ما من أحد سيعلم من أنت. ولكن الأمر يصدق أيضاً على المختطفين، والعاملين في دعارة الأطفال، والإرهابيين، الذين ستصبح حياتهم أكثر يسراً وأماناً بأدوات كهذه.

إن هذه الهموم لم تكن مصدر قلق لزعران الشّيفرة. بل على العكس تماماً، إذ أنهم كانوا شديدي الحرص على بيان الأسباب التي تجعل تقنيات الغفلية موضوع خلاف وجدل. وكان المثال الجيد على ذلك، إعلان تيم ماي

عن تأسيس مشروع تجاري، أطلق عليه اسم بلاك نيت (الشبكة السوداء). وبالطبع، لم يكن للمجموعة وجود. بل كانت تجربة فكرية قرَّر طرحها للنقاش في اجتماع لزعران الشيفرة، لكنَّه بعدئذ قرَّر إطلاقها مغفلة على الشبكة. ويقول ماي: «لقد أرسلتها عبر مدوري الرسائل لإضافة لمسة من التوابل إليها». ولم يكن تيم ماي بالتأكيد يمانع في الإعلان عن معتقداته على الملأ (كان يوقع بريده الإلكتروني عادة بقائمة من أشكال العذابات التي تقشعر لها الأبدان «فوضى التشفير، النقد الرقمي، الشبكات مجهولة المصدر، اسم مستعار رقمي، الأسواق السوداء، انهيار الحكومات»).

كانت بلاك نيت، عرضاً مسرحياً هجومياً لتلك الاهتمامات. بدأت الرسالة «لقد استلفت اسمك اهتمامنا. ولدينا ما يحملنا على الاعتقاد، بأنَّك ربما كنت مهتماً بالمنتجات والخدمات التي تقدّمها منظمتنا الجديدة بلاك نيت. إن بلاك نيت تعمل في البيع، والشراء، والمتاجرة، وعدا ذلك فهي تتعامل بالمعلومات بكافة أشكالها». ويمضي العرض ليشرح بأنه بفضل كريبتوجرافيا المفتاح العام، قامت سوق سوداء رائعة للبيانات حيث يمكن للمرء أن يحصل على أو يبيع أي شيء من أسرار التجارة والصفقات إلىٰ مخططات صواريخ كروز دون أي خطر من اكتشاف هويته. وأطراف الصفقات هذه لن يكونوا معروفين لبعضهم البعض، ولا حتَّى لبلاك نيت. وغني عن القول، أنَّه ما من أحد يملك أن يعلم من يقف وراء بلاك نيت:

إن موقعنا في الفضاء المادي غير ذي أهمية. فالمهم هو موقعنا في الفضاء التخيلي. عنواننا الأولي هو مفتاح بي جي بي لموقع «بلاك نيت» ويمكننا أن نتواصل (يفضل عن طريق سلسلة من مدوري الرسائل المغفلي الاسم) عن طريق تشفير رسالة باستخدام مفتاحنا العام (المذكور أدناه) ووضع هذه الرسالة في واحد من مواقعنا العديدة في الفضاء التخيلي الذي نرصده.

بالإضافة إلىٰ ذلك ادعت بلاك نيت بالتعامل بالمال، وعرضت القيام

بإيداع مجهول المصدر في البنك الذي تختاره. ويمكنك التعامل مع بلاك نيت باستخدام نقد حقيقي، أو «اعتمادات مشفَّرة»، وهي عملة بلاك نيت الخاصة والمتداولة داخلياً (يمكن استخدامها في أي نوع من صفقات المعلومات السرِّيَّة التي لا يمكن تعقّبها ولك أمر اختيارها). ولم يكن لبلاك نيت أي أيديولوجيا خاصة بها، ما عدا قولها: «إننا نعتبر الدول ـ الأمم، وقوانين التصدير، وبراءات الاختراع، واعتبارات الأمن القومي، وما شابه، على أنها بقايا حقبة ما قبل الفضاء التخيلي».

ابتهج ماي، لقبول الكثيرين بإعلان بلاك نيت بمعناه الظاهر، وخاصة أن أنباء عنه قد تسرّبت إِلىٰ أبعد من مجتمع الشيفرة، وإِلىٰ عالم أكثر ميلاً للفزع عموماً. على الرغم من أن بلاك نيت كانت وهمية، فإن ماي كان يعتقد أننا سوف نرى في المستقبل مشاريع مشابهة. ولم يقلقه ذلك على الإطلاق، فالناس عملاء أحرار، ومسؤولين عن أنفسهم. وقد قال: «إذا مات أشخاص نتيجة لذلك. . . إيه! إنني لم أعمل على إيذائهم».

على العموم، لقد وضعت التجربة، علامة استفهام صارخة على فلسفة زعران الشّيفرة. ربما كانت فوضى التشفير حتَّى الآن مجال عمل كتاب الخيال العلمي، لكن الأدوات التي ستجعلها أمراً حقيقياً كانت في الطريق. وعندما وُضع هذا العتاد الرقمي موضع الاستخدام، يمكن لألف شركة مثل بلاك نيت أن تنشأ. بالتأكيد كان ذلك أمراً تنبه إليه، من هم وراء السياج الثلاثي، وكذلك في مقر قيادة مكتب التحقيقات الفيدرالي أيضاً. هل كانت المسألة تنذر بقيام حركة يجب وضع حد لها؟ إن المؤسَّسة كانت قد بدأت تفكّر في ذلك.

وقد أقر دان باركر الخبير في شؤون الأمن، أننا بفضل قدرات التشفير بات «لدينا القدرة على التمتع بسرِّيَّة تامة مئة بالمئة. لكن إذا استخدمنا هذه السرِّيَّة فلست أعتقد أن المجتمع يستطيع الاستمرار في البقاء».

رقاقة المقراض

إن مبتكر رقاقة المقراض Clipper Chip، كان شبحاً من حيث لم يقصد. كان كلينتون بروك شغوفاً بعلم الفلك. فدرسه في جامعة ييل في أواخر الستينات، وأراد أن يتخذه مهنة له، بعد أن ينهي خدمته الإلزامية في البحرية. وما عهد إليه بأداء واجبه العسكري في المحيط الهادي، أخذ يعد لانتقال زوجته وأولاده الصغار إلىٰ هاواي وأن يبحر على متن إحدى السفن، بعد تعيينه ضابط اتّصالات فيها. ولم يكن مدركاً يومئذ أن جماعة معينة في وكالة استخبارات، كانوا يعدون له خططاً أخرى.

كان بروكس، قبل بضعة أعوام، قد عُيِّن في موقع مجهول بالنسبة له ليقضي خدمته الإلزامية الصيفية؛ كان ذلك المكان فورت جورج ميد. فانتقل بسيارته إلىٰ ماريلاند، متوقعاً أن يجد قاعدة عسكرية نموذجية. غير أنه بدلاً من ذلك وجد حراساً غامضين يوقفونه عند مدخل مكان بدا وكأنَّه بناء من أبنية المكاتب الحديثة وسط أرض قفراء. وأخبره هؤلاء أن دخول المكان محظور، إلاَّ لأولئك الذين يحملون تصاريح أمنية عليا. ومما فاجأه، ورود مكالمة هاتفية تفيد بأنَّه قد منح لتوه هذا التصريح. أهلاً بك يا كلينت بروكس في وكالة الأَمن القومي. ولعله حسب أن مهمته هذه مجرد فاصل في سياق خدمته العسكرية،

ومن الواضح أن رؤساءه قد لاحظوا قدراته، وقدَّموا له بديلاً عن الخدمة في البحرية. وكان في هذا العرض ما فيه من الإغراءات، إذ لم يعد بوسعه البقاء في الولايات المتّحدة فحسب، بل سيتاح له أيضاً إرضاء حاجاته على نحو أعمق، فرصة لإشباع أشواقه الكونية، إلىٰ حد ما، بأن يعمل في أقمار استطلاع في غاية السرِّيَّة. ولن يكون قادراً، بالطبع، على إطلاع الأصدقاء والجيران والأقارب على العمل الذي يقوم به، لأنه حتى اسم مؤسَّسة الأقمار الصناعية كان يحاط بالكتمان أكثر من اسم الوكالة [وكالة الأَمن القومي] التي ينكر الجميع وجودها. غير أن العرض بدا جيداً لبروكس. وهكذا رفض المهمة المعهودة إليه على ظهر السفينة بويبلو، سفينة التجسّس التي قدر أن يستولي عليها الكوريون الشماليّون بعد بضعة أشهر، في 23 كانون الثاني/ يناير 1968. إذن لسوف يعمل في الوكالة التي لم يكن ليجرؤ على النطق باسمها.

بعد أربعة وعشرين عاماً، أصبح كلينت بروكس نائب المدير المساعد في الوكالة التي صار الآن يجاهر باسمها بالفعل. ووجد نفسه وسط أزمة تتصل بالمهمة التي تأسّست وكالة الأَمن القومي من أجلها: صعود الكريبتوجرافيا الشعبية. وفي أحد الأيام من أواخر ربيع عام 1992، مضى الرجل إلىٰ مكتب مستشار عام للوكالة، عُيِّن حديثاً فيها، ليطلب منه المساعدة في حملة كان يأمل في أن تساعد الوكالة على اجتياز هذا التطور الخطير.

جرت العادة على أن يتم تجنيد، المستشار العام لوكالة الأَمن القومي من خارج ملاكها، وكان هذا محام حسن الإطلاع على العمل الحكومي، لكن ليست له خبرة تُذكر في شؤون الاستخبارات، حسبه أن يستطيع التلاؤم مع البيئة المغلقة داخل السياج الثلاثي، ويظل على إدراك بالعالم الواقع خارج السياج. وكان بوي إنمان أول من خطر بباله أن عقلاً قانونياً حصيفاً انتزع لتوه من وسط الإهمال يستطيع أن يرعى أعمال الوكالة على أحسن وجه، ويقدم مستوى من النظرة الشمولية قد يقصر عنها شبح موظف. ومنذ أن قام محامو إنمان

بمساعدته في تقصي المشكلات، المتصلة بأبحاث الشّيفرة في الجامعات، كان ثمة سلسلة من المحامين الأذكياء، والشباب نسبياً قد شغلوا هذا المنصب مدة سنتين، ثم انتقل كل منهم إِلىٰ عمل آخر.

كان ستيورات بيكر يناسب هذا القالب. ولد بيكر عام 1947 ونشأ خارج ديترويت، والتحق بكلية الحقوق في جامعة كاليفورنيا بلوس أنجليس، وعمل كاتباً لدى قاضٍ فيدرالي، ثم مارس المحاماة في مكتب ستيبتو وجونسون، وهو واحد من أبرز مكاتب المحامين في العاصمة. وعمل بضع سنوات في وزارة التعليم في عهد جيمي كارتر، ثم عاد إِلىٰ مكتب ستيبتو. ولما تم ترشيحه لوظيفة وكالة الأَمن القومي، تردَّد في قبولها، وسأل أحد أصدقائه العسكريين: «هل أقبل بها؟» فأجابه صديقه: «هل ثمة عمل أفضل يمكنك القيام به من أجل خدمة بلادك؟».

لم يكن قد مضى شهر واحد علىٰ تسلّم بيكر لمنصبه الجديد عندما زاره كلينت بروكس. وكان جلياً أن الموظف العتيد في وكالة الأَمن القومي والنحيل ذو الفك المربع ـ كان مؤمناً حقيقياً ـ لكن بماذا؟ وقبل أن يتحدَّث، وضع بروكس قارورة كبيرة من شراب آدفيل على مكتب بيكر. وقال: «سوف تكون بحاجة لهذا».

بعد ذلك، عرض بروكس قصة كيف أصبحت الكريبتوجرافيا شعبية بحذافيرها. وأخبر بيكر عن معيار تشفير البيانات، والشّيفرة المنيعة التي غدت أكثر انتشاراً مما توقعت وكالة الأَمن القومي، وتطور المفتاح العام، وخوارزمية رسا، والمشكلات التي تُعاني منها الوكالة مع جماعة المشتغلين بالكريبتوجرافيا الجُدد والتي أدَّت إِلىٰ تعرّض عملية مراجعة الأبحاث قبل نشرها للخطر. ثم قال: والآن إن الفكرة القائلة بأنَّك تستطيع السيطرة على الأمور بالتدقيق في الأبحاث العلمية لم تعد مناسبة: فشركات مثل آر إس إيه تبيع الشّيفرة على

نطاق تجاري. كان بيكر يستمع مشدوهاً. وأراد أن يعرف: كيف تركتم ذلك الأمر يفلت من أيديكم؟

أوضح بروكس أن الأمر لم يكن بهذه السهولة، فوكالة الأَمن القومي تضطلع بمهمتين أولاها طبعاً، حل رموز الرسائل المشفَّرة، وتزويد بقية أَجهزة الحكومة بالكثير من المعلومات الاستخبارية ذات الأهمية البالغة لها. أما المهمة الأخرى فهي تزويد الولايات المتّحدة بأفضل ما يمكن من الشفرات. وداخل السياج الثلاثي كان يشار إِلىٰ هذه الثنائية بـ «التوازن»، وهذا يعكس، بلا ريب، تساوي كلتا المهمتين في الأهمية. وكان كلينت بروكس هو رجل التوازن في الوكالة. وكان تحقيق التوازن عملاً لا ثناء فيه ولا شكر، لأن التقدم في إحدى المهمتين، قد يضر بالمهمّة الأخرى أحياناً. في الماضي، على الأقل، كانت النقاشات محصورة داخل القلعة، لكنها الآن تجري في قاعات الكونغرس وعلى صفحات النيويورك تايمز. وفي غضون ذلك، كان شبح التشفير الواسع الانتشار مثل قطار خرج عن مساره مندفعاً ليس نحو وكالة الأَمن القومي وحسب بل نحو المجتمع بوجه عام أيضاً. ومثلما فعل زعران الشّيفرة، أنعم كلينت بروكس النظر في المستقبل ورأى الشّيفرة تنتشر في كل مكان. لكن بينما تقبل ثوار الشّيفرة هذه الرؤية بسرور، فإن بروكس فهم أن هذا الواقع الجديد، ينطوي على كارثة محتملة، إذا لم تتكيّف الوكالة معها.

تلك كانت حقيقة قاطعة لا ريب فيها، راح بروكس يبشّر بها لسنوات عديدة، وكانت تصطدم في البداية بآذان صماء. وخلال معظم فترة الثمانينات، بعد تلك المناوشات الأولى بين المدير إنمان وأكاديميي الشّيفرة، فإن غالبية العاملين في الوكالة لم يكن يعنيهم كثيراً احتمال أن يكون للكريبتوجرافيا الشعبية كبير أثر عليهم. وكانوا مطمئنين إِلىٰ أن الأمور ستظل تحت السيطرة بفضل قوانين التصدير الصارمة فهي الضامن ألا يغادر شيء بقوة معيار تشفير البيانات دون قيود. وفي أوج الحرب الباردة، كان الكونغرس يقدّم للقلعة كل ما تطلبه

على الدوام. ومع أن الأمر لا يخلو من أن يطلع من أهل الدار، بين الحين والآخر بالنذير بنبوءة أحد العلماء بانتشار الشّيفرة في أوساط التجارة على نطاق واسع في غضون عامين أَو ثلاثة، دون أن يبدو أنَّها ستتحقق. وهكذا كان من اليسير أن يعتقد المرء أن هذه النبوءة قد لا تتحقَّق أبداً. لكن بروكس كان يعلم أن الأمور تجري عكس ذلك. وابتداء من عام 1988، توصل إِلىٰ فهم الاتجاه الذي كانت تأخذه الإنترنيت وأدرك أن الخطر ماثل حقيقة هذه المرة. لكن رؤساءه ضحكوا عندما حاول أن يعظهم حول الخطر القادم. وكانوا يقولون له: أي خطر تتحدَّث عنه؟ إننا الكربتوجرافيون الوحيدون، وليس في الميدان سوانا! وهذه تكنولوجيا عسكرية، وليست شيئاً يرغب الناس في استخدامه! ولكن حينما أضحت ثورة الإنترنيت جديرة بالتصديق، وشرعت شركات مثل لوتس، بوضح برامج تشفير مثل رسا ضمن منتجاتها، تحقَّقت الوكالة على أعلى مستوياتها من وجاهة رأي بروكس. ولذلك كان تكليفهم إيَّاه بإيجاد حل لهذه المعضلة. ولقد خرج بروكس بالحل.

كان هذا هو السبب الذي حمل كلينت بروكس، على القيام بزيارة لستيوارت بيكر، ومحاولة إشراكه في الخطَّة. وأوضح له أن ثمة مخرجاً من الورطة... وهو حل لا يقدّم للجماهير شيفرة منيعة توفر حماية لا مثيل لها سابقاً وحسب، بل يحفظ للحكومة كذلك القدرة على حيازة النص الواضح الأصلي للمحادثات والمراسلات. والواقع، أنه خلال السنوات الثلاث الأخيرة، كشف بروكس، عن أن وكالة الأَمن القومي تعمل على ابتكار مثل هذا البرنامج. وكان يقتضي ضمناً توفير تقنية تُعرف باسم وديعة المفتاح Key Escrow.

كان المشروع قد بدأ في عام 1989. وكان بروكس بوصفه رجل التوازن في فورت ميد يقدح زناد فكره ليكتشف طريقة للتوفيق بين مطلبين متعارضين: الحاجة إِلىٰ شيفرة عامة منيعة وحاجة الوكالة إِلىٰ طريقة للوصول إِلىٰ الرسائل

الواضحة. وكان جلياً أنَّه ليس هناك من حلّ كامل. وكان الهدف الذي يسعى إليه هو تحقيق التوازن المناسب، بما يتيح لمستخدمي المعلومات غير المحظورة سواء داخل الحكومة أم خارجها درجة قوية من الأمن، لكن ليس إلىٰ حد انتهاك أمن الجمهور. وفي الوقت الذي كانت فيه وكالة الأَمن القومي قد شكَّلت مجموعة العمل المختصة بالكريبتوجرافيا بالاشتراك مع المؤسَّسة القومية للمعايير والتكنولوجيا وفقاً لمذكرة التفاهم الموقعة بينهما. وقد وجد بروكس في راي كامير مدير المؤسَّسة القومية للمعايير والتكنولوجيا بالوكالة أخاً روحياً له، فراحا يمضيان الساعات الطوال، في استعراض جوانب المشكلة معاً، ويسبران النواحي التقنية، وحتى الفلسفيَّة لسياسة الشّيفرة.

وفي إحدى مناقشاتهما الأولى، توصّل كل من بروكس وكامير في وقت واحد إلىٰ ما يشبه الكشف: إن استخدام التشفير سيكون له تأثير عميق على حفظ الأَمن والنظام، وخاصة من حيث قدرته على مواصلة التنصّت عبر الأسلاك. وشرعا في زيارة أشخاص معينين في وزارة العدل ومكتب التحقيقات الفيدرالي، ولم يكن لدى أي من هؤلاء أدنى معرفة بالمشكلات التي ستعرض لهم مستقبلاً. وعندما كان بروكس أَو كامير يخبرهم أن جميع إجازات التنصّت في العالم قد لا تفيدهم عندما يستخدم المحتالون التشفير، كانوا يقابلون هذه الأقوال بالدهشة. والمسؤولون عن تطبيق القانون يسألون: أليس بإمكانك مساعدتنا؟

إفترض بروكس ذات مرّة، أن الحل ربما يكمن في عملية تضليل جبّارة. فبإمكان الوكالة ابتكار نظام تشفير قوي، إلىٰ الحد الذي يحمل الشركات التجارية على إدخاله بين منتجاتهم، وتصديره إلىٰ كافة أنحاء العالم. لكن الوكالة ستبني في داخله «باباً سرياً»، ليتيح لها استخلاص النصوص الواضحة من البث المشفّر خفية. لكنه بعد أن تروى في الأمر ضرب صفحاً عن تلك الفكرة الخطرة والمشكوك في قانونيتها. وإن مشروعاً كهذا يستلزم الحصول،

على رسائل غير مشفَّرة من مواطني الولايات المتّحدة. وقد تكون قادراً على تبرير باب سري لتستطلع أخبار الأجانب وتتطفل عليهم، ولكن إذا ما اكتشف الكونغرس أَو كاتب من كتّاب التحقيقات، بأن وكالة الأَمن القومي، قد أطلقت خطة مراقبة سرِّيَّة على الأمريكيين، فستبدو لجنة السيناتور تشيرتش أمراً سهلاً.

وهكذا قضى بروكس ليالٍ بكاملها لا يغمض له جفن، ليستحضر في ذهنه فكرة أخرى. وفي إحدى تلك الليالي، لاح له وميض. فقد وجد أن بالإِمكان الوصول إلى حل وسط يمكن أن يرضي الجميع. ففي العالم الحقيقي نجد أن مذكرة التفتيش، تجبر مشتبهاً به في جريمة على تقديم تركيبة مفتاح الخزينة للسلطات. ولماذا لا تتم ترجمة ذلك المفهوم في عالم الاتِّصالات والكومبيوتر؟ فإذا ما ابتكرت نظاماً يمكنك بصورة خاصة من الحصول خفية على نسخة طبق الأصل عن مفاتيح التشفير وتخزينها في مواقع مأمونة، فإنَّك ستكون بالضرورة محتفظاً بتركيبات الأقفال بشكل وديعة غير متاحة لأحد سوى أولئك الذين لهم الحق باستعادتها. وبإمكان هؤلاء بما لديهم من سلطة قانونية ـ مذكرة تفتيش من قاضٍ أَو مجموعة مفهومة من معايير الأَمن القومي ـ الحصول على المفاتيح من موقع التخزين الموثوق به. ومتى كان الوصول إليها مضموناً فليس ثمة مشكلة في أن يسمح للتشفير ذاته أن يكون قوياً مثلما يرغب الجميع. ولتجعله غير قابل للتفكيك! وإذا ما كان مكتب التحقيقات الفيدرالي أَو الشرطة بحاجة للمفتاح، وتم نيل موافقة القاضي، عندئذ سوف يتوفَّر لديهم الشيء الذي يتمكنون به من حل الشّيفرة، وكأنَّهم كانوا المتلقين المقصودين باستلامها.

وبالنسبة لبعض من في الوكالة، كان المشروع بدعة، فقالوا: «إنّك سوف تضع باباً سرياً في نظام التشفير. . . ثم تخبر الناس عنه؟» لكن كشف السر كان جزءاً بالغ الأهمية في رؤية بروكس. لقد كان يريد حقاً لهذا المشروع الجديد أن يبدأ مناقشة شاملة في البلاد حول الكريبتوجرافيا. وكان يذهب إلى الاعتقاد بأنَّه

عندئذ وحسب، سيكون بالإمكان إقامة مشروع الوديعة، الذي يتطلب بنية تحتية معقَّدة. ولما كانت الحكومة غير حريصة على وضع يدها على الرسائل المشفَّرة، فإن الطريق سيكون حراً وواضحاً باتجاه غطاء عالمي من الشيفرة، مع تنظيم توزيع المفتاح العام، وتوقيعات رقمية معيارية، وتشفير آلي للرسائل. وسيثير المهووسون بالسرِّيَّة، وحبك المؤامرات جحيماً إزاء فكرة المفاتيح الوديعة. لكن إذا ما عرضت جميع القضايا على الملأ، وتمت مواجهة الأخطار جميعها، وحدّدت جميع الفوائد، فمما لا ريب فيه أن العقلاء من الناس بإمكانهم أن يروا أن هذه الخطة، هي الطريق الأفضل لحماية اتِّصالاتنا دون أن نضحي بأمننا. وعلى أية حال، ماذا كان البديل؟

وبالطبع، لو قُيِّض لمشروع كهذا أن ينطلق، فإن على وكالة الأَمن القومي نفسها، عندئذ، أن تتغيّر، وتعدّل من تركيز اهتماماتها بحيث تعمل في عالم ما بعد الحرب الباردة المحوسب والمشفّر إلىٰ أبعد الحدود. فالشدة التي ما تزال القلعة تحتفظ ببرقعها من التكتم والسرِّيَّة لم يعد مناسباً. وإذا ما كان الناس سيقبلون فكرة متطرفة كهذه، فينبغي على وكالة الأَمن القومي أن تنال ثقتهم. وهكذا كان من الضروري عرض المناقشات حول الكريبتوجرافيا أمام الجمهور، ليطأ مناطق كانت ذات مرة أرضاً محرَّمة بصدق قاس ومؤلم.

وفي آخر الأمر حصل بروكس على الموافقة لمتابعة خطته، لكن فكرته القائلة بوجوب تعاون وكالة الأَمن القومي مع الجمهور استُقبلت بارتياب أَو ما هو أسوأ من ذلك. ووجد نفسه يجادل كالمتشائم المشوش الفكر. وحالما قابل بروكس أعلى المسؤولين في وكالة الأَمن القومي، قال: «يجب أن تكون هذه سياسة قومية». وعندما طلب منه المدير المساعد أن يزيد في الشرح، أجاب: «هذا ليس حكماً يمكن أن يصدره مدير وكالة الأَمن القومي أَو لجنة من المعاونين. . . إن تعريف مصلحة البلاد مسألة تقدير، حكم قيمة. ولا بد أن يكون رئيس الولايات المتّحدة هو صاحب القرار فيها. المسؤول الذي يتحدَّث

إلىٰ ناخبيه مباشرة! ولقد اعتقد أقرانه بأنَّه بالغ في تصوراته، إذ كان موقفهم؛ هذه وكالة الأَمن القومي، ونحن لا نقوم بعمل كهذا.

وفيما كان ينتظر أن تتخذ المناقشة العامة شكلاً معيناً، كان بروكس يعمل بجد مع وكالات أخرى، من أجل إقامة بنية لخطة وديعة المفتاح الطموحة التي يعدها. وبسبب من مذكرة التفاهم، طبعاً، فإن على الوكالة أن تطور الخطة مع المؤسَّسة القومية للمعايير والتكنولوجيا. لكن ذلك لم يكن مشكلة تُذكر. فقد كانت مجموعة العمل التقني المشتركة تعمل على وضع الشّيفرة العامّة، منذ أول اجتماع لها في آذار/ مارس من عام 1989، وخاصة على خوارزمية التوقيع الرقمي. وكانت الشّيفرة العامة تعرف ضمن المجموعة بالقضية الأولى.

أما الطرف الثالث في المناقشات فقد كان مكتب التحقيقات الفيدرالي. ذلك أن الإنذار المبكر الذي أطلقه كل من بروكس وكامير أيقظ الاهتمام لدى المكتب: ففي عام 1991 كان المدير وليام سيشونس قد كتب إلىٰ وزير الدفاع ديك تشيني حول أمن الكومبيوتر، مشيراً بجلاء إلىٰ أن وكالته ترغب في أن يكون لها صوت مسموع في تحديد السياسة. واتضح أن مكتب التحقيقات الفيدرالي سوف يتخذ حقاً الخط الأكثر تشدّداً في المسألة.

وبالطبع فإن وكالة الأَمن القومي، نهضت بأعباء الجانب التقني. وبحلول عام 1990، كان ثلاثون مختصاً بالرياضيات لديها، يعملون على معالجة المسألة. وقد استقر رأيهم سريعاً على الأساس الوطيد الذي يستند إليه النِّظام، خوارزمية تشفير متينة كانت موضع دراسة ونقاش من فورت ميد لمدة سنتين، يرمز إليها باسم سكيبجاك Skipjack الوثاب [نوع من سمك التونة هـ. م] وكانت كتلة تشفير مثل معيار تشفير البيانات (ديز) لكن أقوى منه. فطول مفتاحها الموصى به 80 بت مقابل 56 لمعيار تشفير البيانات؛ وكانت تستخدم 32 دورة استبدال بدلاً من 16 دورة التي يستخدمها معيار تشفير البيانات. (ويلوح كذلك أن ثمة المزيد من الأسباب التقنية الحاذقة لتفوق الوثاب، لكن بالطبع، كانت

وكالة الأَمن القومي، تنفر من الكشف عنها). ولئن حاول بروكس أن يبرهن أنَّه من المناسب في هذه الحقبة الجديدة أن يتم الكشف عن الخوارزمية ـ وأصر، في الواقع، على أنَّهم إذا ما أرادوا التغلّب على منتقديهم، فسيضطرون إِلىٰ نشرها، إلاَّ أنه لاقى مقاومة قوية. فلن تسمح الوكالة مطلقاً لأعدائها بالدخول، إِلىٰ ما هو أشبه بدورة متقدمة في كتابة الشّيفرة. ذلك أن الأمور لا تسير على هذا النحو في القلعة.

كان الوثاب، مع ذلك، مجرد مكون واحد لما تطلق عليه وكالة الأَمن القومي القمة Capstone، والذي كان نظام مفتاح عام كامل يتضمن معيار التوقيع الرقمي. وبالطبع، كان هذا المشروع بالأخص ينطوي على تعقيد إضافي آخر: كيف يمكنك أن تطبّق نظام الوديعة؟ يجب عليك أن تكتشف طريقة تعزل بها نسخة من كل مفتاح وترسل تلك المعلومات إِلىٰ مكان آخر ليتم تخزينها. وبحلول عام 1991، استقر رأي وكالة الأَمن القومي على أن محاولة القيام بهذا العمل في برمجيات محفوف بالكثير من المخاطر ـ وخشيت أن يتمكّن عدو ما من تغيير الرمز لإضعافه من الداخل ـ وخلصت إِلىٰ استنتاج مفاده أن الطريقة الأفضل تتمثّل بأن توضع المسألة كلها على رقاقة كومبيوترية لا يمكن العبث بها. وتم التعاقد مع مقاول متمرس يقوم بمشاريع لحساب وزارة الدفاع في تورانس بكاليفورنيا يدعى مايكوترونكس، ليقوم بتصنيع الرقاقات.

وكان النِّظام ذاته، يعمل بإدخال عدة مكونات جديدة في المعادلة الكلاسيكيَّة حيث تقوم أليس بكتابة الشّيفرة وبوب بحلّها. وكان أحد هذه المكونات «معرّف الرقاقة الفريد» وهو عدد مكافئ لمفتاح الرقاقة الفريد المخصّص لرقاقة واحدة. ولكل جهاز ـ سواء كان كومبيوتراً أَو ربما هاتفاً ـ معرّف الرقاقة الفريد ومفتاح الرقاقة الفريد الخاص به.

وحينما يرغب شخصان بالاتصال ببعضهما بصورة شخصية، فإنَّه يتعيَّن على كل منهما أن يكون لديه إحدى هذه الوسائل، إذا شاءا مثلاً إجراء مكالمة

هاتفية على نحو لا يدع مجالاً لأحد للتنصّت عليها، فإن عليهما أن يمتلكا أجهزة هاتف ذات خصائص تكنولوجية معينة. ومتى تم الاتصال بين الطرفين، قام الجهازان بتحويل المكالمة بين الطرفين، إلىٰ إشارات رمزية (بواسطة طريقة ديفي ـ هيلمان للتبادل) من أجل حساب مفتاح متماثل جديد، يدعى مفتاح الجلسة. وباستخدام الوثاب يمكن لذلك المفتاح، أن يشفّر الأصوات التي يطلقها كل متحدث عندما تغادر تلك الأصوات جهاز الهاتف، ويفكّك تلك الأصوات عندما تنبثق من الهاتف الآخر. ولكن مع المحادثة المشفّرة فإن أَجهزة الهاتف سوف تبث مجموعة أخرى من البتات تدعى مجال مدخل حفظ النِّظام LIAF Law Inforcement Access Field. (وكان قد دعي أصلاً مجال استغلال حفظ النِّظام، لكن تم تغييره إلىٰ عبارة أقل مدعاة للضيق). ويمكن توليد مجال مدخل حفظ النِّظام، بمجموعة من الحسابات تشتمل على مفتاح الجلسة، ومفتاح الرقاقة الفريد، ومعرّف الرقاقة الفريد، ملفوفة مع عنصرين هامين: نسخة مشفَّرة من مفتاح الجلسة، ومعرّف الرقاقة الفريد. وهذه المكونات جميعها سوف تخضع لمزيد من التشفير بواسطة مفتاح العائلة.

لذلك كيف بوسع المسؤولين الحصول على هذه المفاتيح؟ الحق أنَّهم يمتلكون أحدها أصلاً، مفتاح العائلة، وهو مفتاح وحيد لا ثاني له في النِّظام كله. وإن الجزء الحرج في المشروع يتمثَّل في الحصول على مفتاح الرقاقة الفريد المناسب، وفي النهاية، مفتاح الجلسة. وهذا يمكن القيام به بواسطة مجال مدخل حفظ النِّظام.

لكن ماذا لو أن أحد المتنصتين تمكّن من التقاط المعلومات الخاصَّة بمجال مدخل حفظ النِّظام؟ إن جهوده سوف تذهب سدى، حتى ولو استطاع عزل معرّف الرقاقة من المجال. ذلك أن كل ما سيقوم به المعرّف، حقاً، هو التعريف. إذ سيشير إلىٰ مفتاح الرقاقة الفريد ضمن قاعدة بيانات واسعة. لكن المتنصتين لدى الحكومة المزودين بكل مفتاح رقاقة فريد في الوجود، وحدهم

الذين يستطيعون الوصول إِلىٰ قاعدة البيانات تلك. إن امتلاك ذلك المعرّف دون وجود طريقة للدخول في تجهيزات الوديعة سيكون أشبه بالحصول على بصمة أحدهم دون الوصول إِلىٰ سجلات الوقائع الجرمية: إذ لا طائل من إخبارك عن الشخص الذي تعرف عنه. لكن بمقدور موظف حكومي أخذ ذلك المعرّف مع أمر قضائي، إِلىٰ تجهيزات الوديعة، ومطابقته مع مفتاح الرقاقة الفريد. ومن ثم يضمه إِلىٰ المفتاح العائلي. إذن هاكم الحل! فلسوف يكون لديك مفتاح الجلسة ـ ويمكن لمحادثة مشفَّرة يكتنفها الغموض، أن تتحوّل إِلىٰ لغة واضحة مباركة، أَو ربما شهادة إثبات جرمية.

وقد أدَّى هذا بدوره إِلىٰ تعقيد آخر: أين تخزن مفاتيح الوديعة؟ وإذا ما تمّ الاحتفاظ بها كلّها في مكان واحد، فستكون بمثابه منجم ذهب لكل نصّاب وجاسوس، بل وموظف فاسد، فحكومة الولايات المتّحدة، وبمقدور أي شخص يملك الدخول أن يحصل على جميع الوسائل الكفيلة بانتهاك سرّيّة كل محادثة مشفَّرة في العالم. وهكذا قرَّر بروكس وزملاءه أن يتم تقسيم مفاتيح الوديعة إِلىٰ قسمين يخزّنان في مواقع مختلفة. ويمكن القيام بذلك بحيث أن الحصول على أحد أجزاء المفتاح لن يوفّر أية فائدة رياضيَّة لاكتشاف المفتاح بأكمله. وحينما يسمح قاض بالتنصّت، فإن الموظف المسؤول عن تطبيق القانون سيقدِّم المذكرة إِلىٰ كلا موظفي الوديعة، ويركّب المفتاح، وبذلك يتمكّن من الإستماع إِلىٰ المحادثات.

وفي أواخر تموز/ يوليو 1991، التقت الوكالات الحكومية ذات الصلة بالموضوع كافة لتعقد اجتماعاً خارج مقراتها في دائرة الأبحاث الهندسيَّة التابعة لمكتب التحقيقات الفيدرالي في كوانتيكو، فيرجينيا، للبحث في البدائل لسياسة تشفير قومية. وقد ألقى كلينت بروكس كلمة الاستهلال في الاجتماع. وهذا ما سجّله أحد الموظفين من الحضور:

قدم هذه [البدائل] ضمن سياق هدف قومي يلبي الحاجة إِلىٰ أمن

كريبتوجرافي تجاري وغير محظور بينما مصالح مسؤوليات الأَمن القومي ومنظمات حفظ النِّظام في أمان. وأطلق على إنجاز هذا الهدف اسم «نيرفانا». [مصطلح في الفلسفة الهندية، والبوذية يعني السعادة المطلقة هـ. م].

لم تصل الوكالات إِلىٰ اتفاق تام. ومن الجدير بالذكر، أن مكتب التحقيقات الفيدرالي دعا على ما يبدو لامتلاك القدرة على فكّ التشفير الخاص به على الفور. أَو في «زمن واقعي» وهذا نهج رأى فيه جماعة المؤسَّسة القومية للمعايير والتكنولوجيا «وحشية وتطفلاً». (إن من شأن اتباع نهج مكتب التحقيقات الفيدرالي أن يملي أوامره بأن تسهيلات الوديعة يجب أن تكون مكالمة هاتفية في أي وقت من الأوقات، وسيرمى بالضوابط ضد سوء الاستعمال من النافذة). لكنهم اتّفقوا جميعاً أن النِّظام المقترح يجب أن يوفّر التشفير للجمهور بينما يتيح لرجال الشرطة والأشباح الوصول إِلىٰ المفاتيح ـ وبشكل أساسي كان هذا هو الحل المقدم من وكالة الأَمن القومي.

بقي مشروع الوديعة مجرد تكنولوجيا، تخطف الأبصار، معدّة وراء السياج الثلاثي، إِلىٰ أن اكتشفت الحكومة كلها سرّه. ولكي يعمل، كان من الضروري، أن يكون كلي الوجود. وكما كان بروكس قد توقّع ـ وأدرك رؤساؤه أخيراً ـ فإن تغييراً شاملاً كهذا بحاجة إِلىٰ الموافقة والدعم الفعَّال من أعلى مستويات الحكومة، وصولاً إِلىٰ الرئيس جورج بوش ذاته. ولكن موعد الانتخابات كان يقترب، والوقت ليس مناسباً لطرح أفكار جديدة قد تثير الجدل على الملأ. وعلى أية حال، بدا أن جماعة بوش لم يكونوا مقتنعين بضرورة القيام بعمل سريع. حسب بروكس أنَّه في عام 1993، بعد عودة بوش إِلىٰ البيت الأبيض، فإن الرئيس المعاد انتخابه، سيكون قادراً على معالجة المشكلة، وهو متحرِّر من القلق إزاء ما قد يفكّر به ناخبوه.

لكن في عام 1992، وقع حادثان لم يكونا في الحسبان، حدّدا مجرى الأمور بشأن مشروع وديعة المفتاح بشكل دراماتيكي. وقد تضمّن الأول مُنتَجاً

مبتكراً على وشك أن يدخل السوق، صندوق زنته اثنتين وعشرين أونصة مرتبط بجهاز هاتف. ولقد أنذر ذلك الرطل والنصف من التكنولوجيا، بأطنان من المشاكل. أما التطور الثاني الذي طرأ، فكان انتخاب رئيس جديد للولايات المتّحدة.

كان الاسم التقني للصندوق إيه تي أند تي جهاز الهاتف المأمون AT & T Telephon Security Device (TSD) 3600 (تي إس دي) 3600. ولعدة سنوات كانت تلك الشركة العملاقة في وسائل الاتّصالات عن بُعد، تزوّد الحكومة بهواتف مأمونة، مستخدمة في ذلك خوارزمية خاصة صمّمتها وكالة الأَمن القومي. وفي عام 1992، قرَّرت الشركة توسيع سوقها إلىٰ خارج الحكومة، وبدأت مبيعات محدودة لمشفّر بيانات صوتية باستخدام خوارزمية تشفير ابتكرها فريق الشّيفرة الخاص بالشركة. وفي ذلك الخريف، قرَّرت أن تواصل ذلك على نطاق أوسع أيضاً ـ بإطلاق هاتف مأمون مصنع ليباع منه بالآلاف. وإذا ما كنت تشعر بالقلق إزاء متطفلين يتنصتون على بيانات حسَّاسة تتضمن ملكية فكرية، ومسائل تجارية، واستراتيجيّات مشروعات عمل، فإنّك ستكون بحاجة إلىٰ واحد من هذه الأَجهزة. ولا ينبغي أن تكون مهندساً أَو جريئاً لتستخدمه. وتدفقت أدبيات الشركة معلنة أنه «يرتبط بسهولة بأَجهزة الهاتف المكتبية أو. . . أَجهزة الهاتف الخليوية، كما أنّه سهل الاستخدام فإنّه قابل للحمل والنقل أيضاً. ومن أجل حماية المكالمات، ما على المستثمر سوى أن يضغط زراً واحداً. فيتم تشفير المكالمة بشكل آلي، وتصبح المحادثة مأمونة». كذلك زعمت الشركة بأن نوعية الصوت على هذا الجهاز، بخلاف الهواتف المشوشة نسبياً التي يستخدمها الجيش، جيدة مثل جهاز هاتف عادي تقريباً.

وما هو أكثر من ذلك، أن الهاتف الجديد هذا يستخدم خوارزمية التشفير الأكثر ثقة لتشفير الصوت: معيار تشفير البيانات تلك الشّيفرة التي كانت ما تزال موضوعاً ساخناً خلف السياج الثلاثي.

كانت وكالة الأَمن القومي، غير راضية عن الاستخدام الجديد هذا للطفل المشكلة الذي كانت قد باركته ذات مرّة. لكن أخبار خطة إيه تي أند تي كانت مصدر قلق أكبر لمكتب التحقيقات الفيدرالي. وكان سبق لوكالة حفظ النِّظام هذه أن تذمّرت من الميزات الجديدة للهاتف، مثل الخدمة الخليوية كانت تزيد من صعوبة القيام بالتنصّت. وارتأت أن الحل يكمن في اقتراح مشروع قانون جديد، يُعرف داخل ضاحية المكاتب ببساطة بـ «الإرسال الهاتفي الرقمي» Digital Telephony. وهذا القانون يلزم [الشركات] بأن يتم تصميم جميع معدات الاتِّصالات الجديدة بشكل يلحظ توفّر ما يساعد على التنصّت. وأن يحظر القانون المعتزم إصداره كل الأَجهزة والخدمات الجديدة التي تحرم الحكومة من فرصة ميسّرة للإشراف والمراقبة. وكان المنتقدون قد أخذوا يولولون في ذلك الوقت. فحسبك أن مشروع القانون الجديد سيكبد صنَّاع التجهيزات مئات الملايين من الدولارات (تكلفة يفترض أن يتحمّلها المستهلك). والأسوأ من ذلك الفكرة الأساسيَّة التي كانت وراء التشريع، التي يقصد بها أن يلف ذنب المتنصتين كلب الاتِّصالات عن بُعد. وبدلاً من تشجيع واحدة من أكثر الصناعات ابتكاراً على إنتاج أَنظمة تدعم نجاح التقنية المتطورة لأمريكا في السوق العالمية، تجد أن الكونغرس سوف يعمد إِلىٰ تقييد التجديدات بالسلاسل والأقفال. ومن أجل ماذا؟ لتبقى أذناه مفتوحتان على حوالي 1000 سلك تنصّت فيدرالي سنوياً، لجمع معلومات يمكن الحصول عليها بوسائل أخرى، مثل أَجهزة التنصّت المخفية أَو المخبرين؟

ومع أن الإرسال الهاتفي الرقمي، لم يأت إِلىٰ ذكر الكريبتوجرافيا على وجه التخصيص، فإن شبح قيود الشّيفرة سيكون سيفاً مصلّتاً على التشريع مثل سيف ديموقليس. وكما كان كل من بروكس وكامير قد بيَّنا لمكتب التحقيقات الفيدرالي، فإن الشّيفرة المنيعة تستطيع أن تستجمع مزايا القانون على أكمل وجه. وحتى إذا ما تم إقرار الإرسال الهاتفي الرقمي، والتزمت الصناعة

بقيوده بإخلاص، فسيكون رجال الحكومة، ودوائر الشرطة الأخرى، قادرين على مراقبة البثّ المُرسل عبر الأسلاك أَو الجو، ولكن ماذا سيحدث بعد هذا؟ إذا كانت الاتّصالات مشفَّرة فإن هذه الأجزاء المعترضة الغالية، لن تكون ما يزيد على تشويش عديم الجدوى. ولقد فهم مدير مكتب التحقيقات الفيدرالي وليام سيشونس الرسالة وتأكَّد من أن رجال الحكومة سيكونون مساهمين في الجهد، الذي ستبذله وكالة الأَمن القومي، والمؤسَّسة القومية للمعايير والتكنولوجيا لمعالجة المشكلة.

أخذ مكتب التحقيقات الفيدرالي يتصرّف الآن على نحو غريب. ها هو جهاز هاتف الإيه تي أند تي الجديد، المصمّم من أجل أن ينقل تكنولوجيا الهاتف المأمون من رمز يشير إِلىٰ المكانة في مكاتب مستشاري الأَمن مجلس القومي إِلىٰ منتج تجاري شائع، يستخدمه مدراء الشركات والهيئات، والمحامون، والعلماء، ناهيكم عن المهووسين بالسرِّيَّة، والنصَّابين، والإرهابيين، ويعلم الله من سواهم. وسيكون وبالاً على حفظ النِّظام... ما لم يكن ثمة وسيلة تمكّن الحكومة من أن تتنصّت بطريقة ما على تلك المكالمات كما كان شأنها قبل التشفير. ألم يكن ذلك ما سبق لكلينت بروكس أن اكتشفه؟ وهكذا فقد سئل بروكس وفريقه ما إذا كان من المحتمل أن تدخل رقاقة القمة في جهاز هاتف إيه تي أند تي. وكانت رقاقة القمة في تصورها الأول أقوى من أن يتحمّلها جهاز إيه تي إس دي 3600 ـ [فالرقاقة] بكل ميزاتها، كالتوقيع الرقمي، تتطلّب طاقة كومبيوترية تفوق ما يستطيع الجهاز القيام به. لكن إذا ما نحتت وكالة الأَمن القومي، بالجهد المتواصل خوارزمية التشفير ومفتاح الوديعة فبمقدورها أن تخرج بشيء يمكن أن يثبت في جهاز الهاتف بدلاً من رقاقة معيار تشفير البيانات.

كان بروكس قلقاً، حتى حينما كان يوافق على إمكان القيام بذلك. فلقد كانت رقاقة القمة حسنة التصميم، وتقدّم حلاً كاملاً. وكان في طرح حل جديد

مجازفة أكبر ـ وللقيام بذلك في الوقت المناسب لخرق هاتف إيه تي أند تي، ينبغي تنفيذه بسرعة كبيرة. ولن يكون هناك متسع من الوقت، لإجراء مناقشة قومية كان يشعر بأنّها أساسية جداً.

لكن مكتب التحقيقات الفيدرالي لم يكن بمقدوره الانتظار. ففي 13 تشرين الأول/ أكتوبر 1992، أجرى القاضي سيشونس اتّصالاً هاتفياً مع المدير التنفيذي في شركة إيه تي أند تي روبرت ألن، وأخبره بمواجهته مشكلة، ثم أوجز له المشكلة والحل: هل ستفكّر الشركة في استخدام رقاقة تشفير وديعة، عوضاً عن نظامها المستند إلىٰ معيار تشفير البيانات؟ وإذا ما وافقت الشركة على ذلك، فبمقدور الفيدراليين تقديم مكافآت كثيرة. وبإمكان إيه تي أند تي الادعاء بأنّها كانت توفر حقاً تشفيراً أقوى، بما أن تفكيك الدخلاء لرموز الوثاب كان أكثر صعوبة من حل رموز معيار تشفير البيانات. علاوة على ذلك، فالمرجح أن الولايات المتّحدة، سوف تسمح بتصدير هاتف وديعة المفتاح هذا. والأفضل من هذا كله كان وعداً للشركة ببلوغ المراد: أي أن تشتري الحكومة آلاف الوحدات لاستخدامها الخاص.

إن الوجه الآخر، طبعاً، سيكون على المشتركين المحتملين، أن يشتروا في ظلّ التسوية الأساسيّة التي استلزمتها الوديعة: سيكون التشفير قوياً، لكن طرفاً ثالثاً ليس موضع ترحيب بالضرورة سوف يكون لديه نسخة من المفتاح.

هل يبدو ذلك مألوفاً؟ إنه الوضع ذاته الذي كان هويت ديفي قد وجد، أنه لا يمكن تحمّله على الإطلاق قبل عقدين من الزمن: الصعوبة التي يجدها شخصان ينشدان علاقة حميمة في حين أن شخصاً آخر في الفراش. ولقد ابتكر ديفي المفتاح العام لتفادي إساءة استعمال العلاقة الكريبتوجرافية. والواقع، أن هاتف إيه تي أند تي كما تمّ تصوّره أصلاً، كان تجسيداً لرؤية ديفي. فلن يكون مستخدمو الهاتف بحاجة لتبادل مفاتيح سرية سلفاً. وعوضاً عن ذلك، سوف يقوم جهازا الهاتف كل منهما في مكانه الخاص بإعداد الحسابات لتبادل المفتاح

حسب طريقة ديفي ـ هيلمان، للاتفاق على مفتاح مأمون من معيار تشفير البيانات يشفّر، ويفك تشفير المحادثة الفعلية. لن يكون ثمة حاجة إِلىٰ أي شخص آخر. إنّك لن تحتاج إِلىٰ شخص آخر. لكن المنحة السخية المقدَّمة لشركة إيه تي أند تي ـ والفرصة السانحة لتفادي المواجهة مع الحكومة ـ كانت رابحة أكثر مما ينبغي بما لا يدع مجالاً لرفضها. ولقد وقَّعت شركة الهاتف على اتفاق: إذا تبنّت الحكومة خطة لجعل وديعة المفتاح معياراً لها، فإن إيه تي أند تي سوف تتخلّى عن مشروعها الذي يستند إِلىٰ معيار تشفير البيانات. وتضع في أجهزتها بدلاً منه رقاقة من تصميم الحكومة. وستكون هذه [الرقاقة] هي النسخة المخففة من رقاقة القمة، مستخدمة خوارزمية الوثاب وميزات الوديعة، لكن بدون التوقيع أَو خوارزميات التجميع. ولها اسم رمزي جديد: المقراض.

قالت متحدِّثة باسم الشركة: «إننا نعلم أن أي قرار لن يحقِّق السعادة للجميع. لكن بصراحة، لقد وفَّرت رقاقة المقراض، مسألة هامة تتصل بحفظ النِّظام وزادت في مستوى الحماية». وعلى نحو أكثر صلة بالموضوع، فإنَّها ضمنت كذلك قدراً من المبيعات، والرضا الدائم لأحد زبائن إيه تي أند تي الرئيسيين، أي حكومة الولايات المتّحدة (في ذلك الوقت، كانت الشركة تفاوض على عقد حكومي تربو قيمته على عشرة بلايين دولار). وإذا ما أضحت وديعة المفتاح سياسة حكومية، فإن إيه تي أند تي سوف تكون قد استقرت بسعادة على متن السفينة.

لكن المقراض كان ما يزال أبعد ما يكون عن اعتماده من الحكومة سياسة رسمية. وكان كلينت بروكس ووكالة الأَمن القومي بحاجة إِلىٰ فرصة أخرى قبل بدء الرحلة نحو النيرفانا. ولقد تحقَّقت الفرصة المنشودة في 3 تشرين الثاني/ نوفمبر 1992 حينما توجهت الولايات المتّحدة إِلىٰ صناديق الاقتراع وانتخب وليام جيفرسون كلينتون رئيساً لها، وألبرت جور نائباً له.

وقد يبدو أمراً منافياً للبداهة الاعتقاد بأن نتائج الانتخابات، جاءت في

صالح وكالة الأَمن القومي. فبعد كل شيء، كان كلينتون ديمقراطياً قضى سني حرب فيتنام، يتحدَّث مناهضاً الصراع بدلاً من أن يقاتل فيه. وإبان الحملة الانتخابية، كان كلينتون قد زار [مجمع الصناعات الإلكترونية] سيليكون فالي، وفي الوقت الذي لم يقطع فيه أي وعود، إلاَّ أنه أشار إِلىٰ أن حكمه سيكون صديقاً للشيفرة الخاصة. ويتذكَّر المدافع عن السرِّيَّة مارك روتنبيرج: «لقد عرض لنا مبلغ سخف، بفرضه قيوداً على تصدير البرمجيات الجاهزة على الرفوف. ولم يقل «التشفير على وجه التخصيص، لكن هذا ما كان يشير إليه بكل وضوح».

ثمة إشارة أخرى إِلىٰ أن كلينتون، قد لا يكون صديقاً لوكالة الأَمن القومي وهذا يعود لطبيعة الأشخاص المحيطين به. مثلاً، كان رئيس فريق ترتيب إجراءات انتقال الرئاسة، عضواً سابقاً في جماعة ضغط تعمل لصالح الصناعات الإلكترونية يدعى جون بوديستا، الذي كان مؤيداً متحمساً لبرنامج الصناعة لتحرير قوانين التصدير. وإِلىٰ جانب بوديستا كان في عداد المحظيين عند كلينتون عدد من الأشخاص الذين بدوا متناغمين مع العلماء وعالم التحكّم الآلي المناصر للشيفرة.

وكان الأبرز من بين أعضاء الفرقة تلك، نائب الرئيس ذاته، أحد المهووسين بالكومبيوتر والذي أناط به كلينتون مهمة اتخاذ القرار النهائي في مسألة الكريبتوجرافيا. والواقع أن وجود آل جور بوصفه الثاني في قيادة الأمة كان ينوّه به على أنّه دليل. على أن فريق القيادة الجديدة كان فرقة تناصر الجرأة وتتطلّع إِلىٰ المستقبل، و«فهمت» نموذج الإنترنيت الجديدة. وكانت خطب حملتهم تدور حول إقامة جسور إِلىٰ المستقبل، لكن رؤية جور كانت لطريق معلومات سريعة لنقل البلاد بل الكرة الأرضية إِلىٰ حال أخرى. ورتّب جور إحضار بعض مستشاري مجلس الشيوخ الأكثر معرفة بالتكنولوجيا إِلىٰ البيت الأبيض للمساعدة في الشؤون الرقمية، مثل مايك نيلسون، وهو جيوفيزيائي، وأستاذ سابق في معهد ماساتشوسيتس للتكنولوجيا، وخبير متمرس في شؤون

طريق المعلومات السريعة. ولقد كتب جون بيري الذي تعرف إليهم بحكم كونه مؤسّساً مشاركاً في مؤسّسة الآفاق الإلكترونية قائلاً: لقد كانوا «عشّاق حرية واعين وأذكياء إلىٰ أبعد حد. إن الكثير منهم لا يسهل قيادهم. وكنت واثقاً من أنّهم بعد انتقالهم إلىٰ مواقعهم بشكل تام، سوف يواجهون وكالة الأَمن القومي، ومكتب التحقيقات الفيدرالي بجسارة».

كان بارلو قد افترض على نحو خاطئ، أن أعوان كلينتون قد عرفوا افتتاحية «المغنوليا الحلوة»، فإنّهم سوف يكونون معفيين من جحيم المحاضرات السرّيّة التي اعتاد صبية الشّيفرة المزينين بالنجوم، على إلقائها في فورت جورج ميد. وخلف السياج الثلاثي، كانت التوقعات على النقيض من ذلك تماماً. فقد أدرك الأشباح أن بيل كلينتون وفريقه من التقنيين المزهوين بأنفسهم كانوا نعمة من الله من أجل خطة الوديعة. ولم تكن المشكلة إلىٰ حدّ بعيد أن جماعة بوش كانوا بشكل خاص ضد هذا المشروع على وجه التحديد. فقد كانوا يناهضون كل ما يتطلب شيئاً من روح المبادرة. وقال أحد المطلعين يصف الوضع: «كان جماعة بوش [الجمهوريون] قد قضوا اثنتي عشرة سنة في السلطة، معظمها مع كونجرس ديمقراطي، وعلموا أن كل ما يمكن أن ينفجر، سوف ينفجر. وعندما تقدم لهم شيئاً، لن تحصل منهم إلاّ على عيون تحدّق... يمكنك أن تشعر بأن كل واحد منهم كان يفكر: «ما مدى تأثير هذا على وضعي؟»».

وعلى النقيض من ذلك، كانت جماعة كلينتون من السياسيين المغامرين، أشبه بمراهقين سلم لهم القياد أخيراً. لقد كانوا يشعرون بسعادة غامرة، أنّه بعد اثنتي عشرة سنة من حكم الديناصور، سنحت لم الفرصة لإصلاح الأمور. كذلك كانوا مهووسين بالتفاصيل، وتوّاقين لاستيعاب الركام الهائل من البنود والهوامش والتوافه التي تجسّد عملية الحكم. اعرض لهم فكرة لتجدهم قد أحاطوا بها، وداعبوها، ومزّقوها إرباً إرباً، واختبروها حتى وجدت أجزاءها

تفرقع، وراحوا يتساءلون كيف بوسعهم جعلها تعمل لصالحهم. كانوا يستمدون الثقة بأنفسهم من إيمانهم بأن نواياهم واضحة، وأنَّه حتى ولو لم تكلل جهودهم بالنجاح، فإن الجمهور سوف يقرّ لهم بالفضل لمحاولتهم القيام بالعمل الصائب.

لم تنتظر القوى التي تدفع وديعة المفتاح، وصول الإدارة الجديدة إِلىٰ البيت الأبيض، قبل أن يصدموا كلاً من كلينتون وجور بمشكلة التشفير. وقد وفَّر هاتف إيه تي أند تي زخماً وقوة دفع لذلك. وفي هذا الصدد يقول ستيوارت بيكر: «فجأة وجدنا أن هذا ليس بالأمر الذي يحتمل انتظار، إعداد بيان موجز منهجي للإدارة الجديدة، وأن ندعهم يلتفتون لتدبير شؤونهم، ويعينوا الوزراء، ويصدروا قراراً في عام 1994». وكانت فكرة جعل جورج بوش يعلن انتهاء البرنامج قبل إخلائه البيت الأبيض قد أُخذت بعين الاعتبار، لكنها رُفضت». وكتب مسؤول في مكتب التحقيقات الفيدرالي إِلىٰ المدير سيشونس في مذكرة أعدّها في أواخر عام 1992: إننا نعتقد بأن المضي قُدماً في تركيب رقاقة المقراض بناء على موافقة الإدارة الحالية أمر يعتوره عقبات محتملة. فماذا لو تسرّبت الأنباء عن رقاقة «قابلة للاستثمار» قبل أن توافق جماعة كلينتون على السياسة بشكل رسمي؟ «وقد يفضي ذلك إِلىٰ دفعهم إِلىٰ التنصل من منهج إدارة بوش السابقة للحيلولة دون وقوع جدل». كان القاضي سيشونس ذاته، الذي بلغ به الخوف من أن يفقد عمليات التنصت الأثيرة على قلبه حد الاهتياج أو من يبلغ مدينة ليتل روك. [عاصمة ولاية أركنساس، مقر الرئيس المنتخب كلينتون هـ. م] ويقول مسؤول حكومي مؤيد لوديعة المفتاح: «لقد أصبحت هذه تتصدّر سلم أولوياته. وكان مقداماً في مخاطبة الفريق الذي يتولَّى ترتيب إجراءات انتقال السلطة، فخاطبهم بقوله: «أيها الشباب، لعلكم قادمون في كانون الثاني/ يناير، لكن يجب عليكم أن تسمعوا هذا الآن». على أية حال، فإن وكالة الأمن القومي، كانت راضية تماماً عن تصدره الحملة. ففي

النهاية، لم يكن الدور المعلن المناط بفورت ميد في الحكومة دعم القرارات السياسيَّة، بل توفير خلفية تقنيّة ومعلومات استخباراتية من ملفاتها.

ولتأطير القضايا، قام مكتب التحقيقات الفيدرالي، بمساعدة من وكالة الأَمن القومي، بإعداد بحث بعنوان «التشفير، حفظ النِّظام، والأمن القومي». وحفلت هذه الوثيقة بسيناريوهات ذات وقع شديد لما قد يحدث، إذا ما تحرّرت الشّيفرة من القيود. وتعرّض البحث إِلىٰ جهاز إيه تي أند تي، بوصفه محرضاً لهذا الهجوم الضاري. لكن البحث ذهب مع ذلك إِلىٰ إمكانية تفادي الكارثة المقبلة. «إن الحل يتمثَّل في رقاقة تشفير، توفر مزيداً من الحماية للسرِّيَّة (قوتها تفوق قوة معيار تشفير البيانات بمليون مرة على الأقل)، غير أنَّها تسمح لمسؤولي حكومة الولايات المتّحدة قراءتها متى أجاز لهم القانون ذلك. . . إن من شأن نظام «وديعة المفتاح» هذا حماية شركات ومواطني الولايات المتّحدة، من انتهاك الأمان الذي يتمتعون به على يد الراصدين المأجورين والمنافسين والحكومات الأجنبية. كما يتيح في الوقت ذاته، للأَجهزة القائمة على حفظ النِّظام ممارسة التنصّت على خطوط الاتِّصال في الظروف ذاتها السارية الآن بمقتضى القانون». ولئن بدا الوصف أشبه ما يكون بدواء عام لمشكلة إن لم نحتاط لأمرها الآن أتت فيما بعد بأعظم الكوارث، فإن البحث عرض لنتيجة واحدة تحمل نذيراً بالشؤم، إن استمرت السياسة الراهنة: إن هذا المفهوم سوف يُهاجَم بقوة، من أولئك الذين يخشون إساءة تطبيق القانون وبالتالي فإنَّهم سيؤثرون الاعتماد على التكنولوجيا على اللجوء إِلىٰ المحاكم من أجل حماية سريتهم». لكن ذلك بدا تزييناً لمقايضة لا تخلو من التبسيط في معالجة الأمور. فكأنما أراد الكاتب أن يحدّد الحل بالخيار بين اثنين: فأيهما تفضل قليلاً من نيران المدفعية المضادة للطائرات من المهووسين بالسرِّيَّة، أم سلاحاً قوياً بأيدي المختطفين والإرهابيين؟

كان ستيوارت بيكر الشخص المسؤول عن القضية في وكالة الأَمن

القومي، وانتهى به الأمر إلىٰ التنسيق، بين الجهود الكثيرة المبذولة لإقناع القيادة الصاعدة بإقرار مبدأ الوديعة. ففي الوقت الذي كانت فيه فورت ميد حافلة بالعباقرة، لم تكن مليئة بالقدر نفسه بأناس يرتاحون بالتعامل مع العالم الخارجي. وكان بيكر قد قطع شوطاً كبيراً في الارتقاء في سلم المراتب، منذ أن زاره كلينت بروكس في مكتبه وأخبره أول مرة عن التوازن. وقد تكونت لديه منذ ذلك الوقت صورة جيدة للمشهد الكريبتوجرافي من وجهة نظر وكالة الأَمن القومي، ورأى كيف تتصل الأمور ببعضها وتتناسق. إنك لا تستطيع فرض ما يستخدمه الناس داخل البلاد ولا يمكنك كذلك إبقاء كل نسخة من برنامج مثل منتهى السرِّيَّة PGP بعيداً عن متناول أي كائن في هذا العالم. لكن في الواقع، لن نجد الكثير من الناس يكلفون عناء البحث عن برمجيات تشفير غريبة مثل منتهى السرِّيَّة واكتشاف طرق استخدامها. كانت القيود المفروضة على التصدير هي الطريقة التي توسّلت بها لإيقاف الشّيفرة الجيدة ـ كل شيء من مستوى معيار تشفير البيانات فما فوق ـ منعت من أن تكون من مكونات الأَنظمة التي يستخدمها الناس كل يوم، وبالتالي، بعيداً عن متناول معظم الأشرار.

كان بيكر يرى في مشروع رقاقة المقراض وسيلة تغني الحكومة عن الاعتماد على القيود المفروضة على الصادرات لاحتواء الشّيفرة. وكان ثمة إشارات بأن الكونغرس قد لا يستمر في دعم الأَنظمة تلك إلىٰ الأبد، وراحت تتعالى الأصوات بين أوساط رجال الأعمال في معارضتهم لها. وكانت المشكلة، أن صناعة البرمجيات كانت قد نمت في بيئة، الأَنظمة فيها قليلة، وأضحت الآن صناعة ضخمة تقدّر بعدة مليارات من الدولارات. وكان الرأي السائد أن طبيعة الأمور تفرض حسمها بالقتال في السوق فيما تبقى الحكومة كياناً ينأى بنفسه إلىٰ حد ما عن التدخل. وبدا أن سريعو الغضب كانوا يعتبرون وكالة التشفير الأولى في العالم خرفة بعض اشيء، ونتاج مصطنع للحرب الباردة، لا علاقة له بواقع الحال اليوم. وكانت فلسفتهم هاكم، التكنولوجيا

تتحقَّق. ولقد شعر بيكر بالهلع ذات مرة حينما أخبره أحد المدراء المساعدين في مايكروسوفت بابتهاج أن بيل جيتس كان سيدخل الشّيفرة في نظام تشغيل مايكروسوفت، وأنَّها ستكون موجودة في كافة تطبيقاته. ومن يهتم إذا كانت ستقوي الإرهابيين أَو تشرّد الأمم؟ كان موقفهم: «إن التشفير ممتاز، لنضعه في أي مكان».

كان بيكر يعتقد في دخيلته، أن هؤلاء السريعو الغضب، ليسوا بعيدين عن الوطنية، وإنما يجهلون المخاطر الحقيقيَّة في العالم. وكانوا يعدّون تصنيف الشّيفرة بموازاة الأعتدة الحربية الثقيلة. لكن إن التنصّت على العالم بشبكة واسعة تقدّر كلفتها بعدة مليارات من الدولارات من الأقمار الصناعية، وقواعد الرادار، وأجهزة التحسّس الأرضية السرِّيَّة، كان عماد السياسة الدفاعية للولايات المتّحدة. هل ثمة طريقة أخرى لتتبع البرنامج النووي لكوريا الشمالية أَو استخدام العراق للأسلحة الكيميائية ضد الأكراد؟ إن الجمهور كان قد سمع تلميحات وحسب عن أهمية تلك «المعترضات»، مثل الإشارات المنتزعة من المكالمات الهاتفية، والتحويلات الرقمية، وحتى بثّ أَجهزة التليفون المتنقل (الووكي توكي). وكان معظمها محظوراً، ويعتبر في غاية السرِّيَّة. لذلك لم يكن هناك صحفيون حينما تجرأ الرئيس بوش ذاته على زيارة فورت ميد (وكالة الأَمن القومي) ليقدم تهانيه الشخصية إِلىٰ مفككي الشيفرة على ما قاموا به من أعمال أثناء حرب الخليج. لكن ما الذي فعله هؤلاء الأشباح على وجه التحديد؟ لو أن الجمهور يعلم. . . .

اعتبر بيكر وزملاؤه المدافعين عن نظام الوديعة، أن من الضروري أن تكون النظرة التي أخذت بها الإدارة الجديدة عن العالم أكثر واقعية وقوَّة. ولا ريب أن التشفير يجب أن يكون جزءاً هاماً من المجتمع المتشابك، لكنك تحتاج إِلىٰ ضوابط، تحتاج إِلىٰ حدود تحترم ولا يجوز خرقها، تحتاج إِلىٰ

طريقة ليسمع الأشخاص الطيبون ما الذي يقوله الإرهابيون، والمحتالون لبعضهم البعض.

في وقت مبكر من الحملة للفوز بأفئدة وعقول جماعة كلينتون، أطلع بيكر وسيشونس ليون فيورث، الذي سيصبح مستشار آل جور لشؤون الأَمن القومي، على الموضوع. ومع أن فيورث كان حذراً، فقد كان بالإمكان أن يرى مؤيدو الوديعة أن حجتهم أصابت هدفها. واعتقدوا أنّه كان ظاهراً على وجهه: الإدراك بأن الحملة الانتخابية قد انتهت وأن جماعة كلينتون سوف يكونون الآن في صراع مع بعض القضايا العويصة جداً. وكانت هذه إحدى تلك القضايا العويصة التي بمقدور وكالة الأَمن القومي، ومكتب التحقيقات الفيدرالي الفوز بها.

ومع تعاقب أيام شهر كانون الأول/ ديسمبر، تواصلت جلسات الإطلاع. وبعيد يوم التولية [حينما يتقلّد الرئيس منصبه رسمياً في 20 كانون الثاني هـ. م] تعرّف آل جور بنفسه على عقيدة وكالة الأَمن القومي من المدير مك كونيل وكلينت بروكس. وكانت ضربة موفَّقة للقلعة. وبسبب من ولع آل جور بالتكنولوجيا، كان يستطيع تقدير براعة مشروع وديعة المفتاح حقّ قدره. ولربما عمد محطّم آلات حديث من الجمهوريين إلىٰ التشويش على تلك التفاصيل، لكن انفتاح جور تجاه الفكرة بدا مقيداً بإدراكه بأن أَجهزة ورافعات البرمجيات قد تعمل فعلاً، وتوفّر حلاً يمنح لكل واحد شيئاً ما.

ما أن تبدّل حال فريق كلينتون ـ جور من الانتقال إلىٰ الحكم، حتى ضاعف جماعة رقاقة المقراض من اجتماعاتهم. وكانت المذكرات تطاير ما بين وكالة الأَمن القومي والمؤسَّسة القومية للمعايير والتكنولوجيا لمناقشة أفضل السُّبل للتنبؤ بالاعتراضات المحتملة والاستجابة لها. وكانوا يعون وجود مشكلة محتملة واحدة، هي إصرار فورت ميد على إبقاء العمل في رقاقة المقراض سرّاً عن الجمهور. ولقد حاول بروكس إقناع زملائه بكشفها للجمهور، لكنّه أخفق في مسعاه. كانت خطته الاحتياطيّة الحصول بطريقة ما، على ضمانات بأن

وكالة الأَمن القومي، لم تضعف الوثاب قصداً خدمة لأغراضها الخاصَّة. وكتب بسرعة مذكرة وجَّهها إِلىٰ مديره في 5 كانون الثاني/ يناير: «إعمل على عقد ندوة من الأكاديميين، من أوساط محللي الشيفرة المختصّين بالرياضيات، لدراسة مستوى الوثاب المحظور، للتأكّد من أنَّه خوارزمية جيدة. فمن هم يا ترى»؟

في غضون ذلك، كان تأثير هذا الوابل من الجلسات اليومية على البيت الأبيض، يزداد باطّراد. وفي الأسابيع الأولى من الحكم، لم يكن كلينتون وجور قد أعلنا انتهاء العمل بالمقراض. بيد أن أعوانهما كانوا قد اقتربوا من الاستنتاج أنَّه ليس ثمة بديل آخر عن هذه الأداة.

كان جون بوديستا في ذلك، الحين أحد أعضاء الإدارة. ولعل لحظته حانت في وقت مبكر جداً، بعيد بداية العهد الجديد حين جاء لزيارته بعض جماعات الضغط المدافعة عن التكنولوجيا المتقدمة. في ذلك الوقت، كان مؤيدو مبادئ الحرية المدنية وجماعة صناعة البرمجيات ما زالوا يأملون بأن تقوم الإدارة الجديدة بعمل مناهض للأشباح ورجال الشرطة وتحرّر أَنظمة تصدير الشيفرة. (ولو أنَّهم كانوا يعملون بأمر رقاقة المقراض لانفجروا). أما بوديستا، فكان لا يزال منبهراً بالألعاب الجديدة في كتبه، عرض لهم جهاز هاتف STU-III الخاص به، وهو جهاز هاتف الشيفرة المعياري، الذي كانت الحكومة قد استخدمته منذ حوالي خمسة أعوام. فسخروا منه وقالوا: «حل حكومي نموذجي مجلجل كما هو عهدنا بها، ولكن هل تعلم ما هو الممتاز؟ إن إيه تي أند تي سوف تصنع جهازاً حجمه نصف حجم هذا الجهاز، وأرخص منه بكثير، وسيقوم بكل ما يقوم به هذا، إنما بصورة أفضل. إننا ننصحك بشراء هذه الأَجهزة!» ومع أن جماعة التكنولوجيا المتقدمة لا يعلمون شيئاً، فإن تعليقاتهم كانت في الحقيقة ترجيع صدى للمذكرات التي كان يتلقاها بوديستا. وما لم تفعل الحكومة شيئاً، فعلى الأرجح أن الأَجهزة اللعينة تلك سوف تكتسح السوق.

وليس مؤدى ذلك، عصبة مؤامرة المقراض في وكالة الأَمن القومي، ومكتب التحقيقات الفيدرالي كانت تعول على ضربة خط لإعادة جماعة كلينتون إِلىٰ جادة الصواب. فقد كانوا يرتبون أوراق اللعب بشكل أساسي، ويعرضون مجموعة محدودة من الخيارات للأغرار. لا تريد أن تفعل شيئاً، وتدع السوق تأخذ مجراها الطبيعي؟ رائع. إذا ما كنت تريد أن تطلق فوضى التشفير، من عقالها فهاكم هي. وحذروهم، ألا تفعلوا شيئاً، يعني أن إيه تي أند تي سوف تبدأ ببيع أَجهزة الهاتف وتعلمون بأن التكاليف سوف تنخفض وستجدون الناس يتحادثون على هواتف مأمونة ويتراسلون ببرمجيات مشفَّرة. وكان الدخان المتصاعد من تفجير مركز التجارة العالمية بالكاد قد تبدَّد. وماذا لو أن كارثة إرهابية أخرى، وربما أسوأ منها، وقعت، وتبين أن الحكومة قد أخفقت في الحيلولة دون وقوعها لأن مرتكبيها كانوا قادرين على الاتِّصال فيما بينهم بشيفرة غير قابلة للتفكيك؟ أتود أن تمنح صدَّام حسين القدرة على استعمال شيفرة ليس باستطاعتنا تفكيكها؟ هيا، ثابروا على ما أنتم عليه، ولا تفعلوا شيئاً. ولسوف تتحمّلون وزر الدماء التي ستسفك. وقد أفزع هذا الطرح جماعة كلينتون.

أما البديل الآخر، والذي كان بعض المتشدّدين في مسألة حفظ النِّظام يطالبون به بإلحاح، فقد كان أكثر تطرّفاً: حظر الشّيفرة داخل الولايات المتّحدة. وفي إحدى المحاضرات التي قدَّمها مكتب التحقيقات الفيدرالي والتي رافقها عرض شرائح منزلقة (سلايد) وجداول بيانيَّة ومؤشّر ليرسم خطاً يبرز النقاط الهامّة، دمج رجال الحكومة أهدافهم المتصلة بالمقراض مع رؤيتهم للإرسال الهاتفي الرقمي. كان العرض يقول بشكل أساسي: إن عدم ضبط الاستخدام المحلي للشيفرة أدّى إِلىٰ ظهور الحاجة إِلىٰ وضع سياسة قومية شاملة على مستوى البلاد تجيز للمستخدمين «الشرعيين» استخدام الشّيفرة لإحباط جهود خصومهم، وكذلك «تكفل للأَجهزة والأَنظمة الكريبتوجرافية

القدرة على التشفير، في الوقت المناسب لتطبيق القانون». إن المعنى المتضمن والذي لا يمكن تفادي استخلاصه هو: يجب حظر أي كريبتوجرافيا غير مطابقة للمعايير، بما في ذلك الأَجهزة والأشياء التي يوزعها المصنّعون الأمريكيون على المستخدمين الأمريكيين. وإِلاَّ نشأ «ملاذ إِلكتروني» لا يحتمل. فلتنسوا استراتيجية استخدام القيود المفروضة على الصادرات لتخفيف ما يستخدمه الناس داخل البلاد. . . لقد كانت أمتنا معرّضة للخطر بسبب من أن أدوات كهذه، كانت متاحة قانونياً لمن يشاء، إذا كان لديه حافز للبحث عنها. ومن غير القانوني السماح بوقوع الأسلحة النووية بيد كل من هبّ ودبّ، كذلك يجب ألا يكون قانونياً وقوع الشّيفرة، في أيدي أولئك الذين سيدمّرون المجتمع بها. ونجد في هذا الرأي ترجيعاً، بطريقة عجيبة غريبة، لصدى قول فيل زيمرمان: «حينما تكون الشّيفرة محظورة، فإن الخارجين على القانون وحدهم سوف يمتلكونها».

ولقد تدبّر جماعة كلينتون مقاومة ذلك المطلب، الذي كان سيثير شغباً في سيليكون ڤالي، ولعله ما كان ليفلت من مقاضاته أمام المحاكم. وكان فريق جور على وجه الخصوص ذا حساسية إزاء الفكرة القائلة بأن طريقة المعلومات السريعة الآخذة بالنشوء كانت بحاجة إِلىٰ حماية لسرّيَّة مراسلاتها. ثم كيف لك أن تفرض حظراً كهذا؟ ماذا يريد هؤلاء من الحكومة أن تفعل، أتراهم يريدون منها الانتقال من بيت إِلىٰ بيت والتفتيش في الأقراص الصلبة للناس، بحثاً عن نسخ من برنامج بي جي بي؟

وبعد أن قُدّم لجماعة كلينتون بديلين مقيتين، طرح عليهم طريقة ثالثة، بدت على النقيض من غيرها، تسوية يمكن للجميع التعايش معها. وفي استعادة للأحداث الماضية والتأمّل فيها، راح أحد المطلعين في الإدارة ينظر إليها على أنَّها مماثلة للخيارات التي قدّمتها جماعة كينيدي بشأن غزو كوبا ـ وهي إما تفادي المشكلة وهذا ينم عن الجبن، وإما عمليَّة عسكرية واسعة النطاق تشيع

الاضطراب وعدم الاستقرار، أو الخطة الأخرى، وهي عملية صغيرة في مكان ما يدعى خليج الخنازير.

تم عرض هذا المشروع على جماعة كلينتون على أنّه مشروع جاهز للتنفيذ والدخول في العمليّة حالما يعطي الرئيس الأمر. حتى التراخي المؤقت كان يعني عند القوم فقدان احترام قاعدة أنصار القانون والنِّظام الذين تحتاج إليهم الإدارة. كان أحد رجال مكتب التحقيقات الفيدرالي الذي يتولى اطلاع جماعة كلينتون على مجريات الأمور، رجلاً ضخماً أنيقاً هو المدير المساعد جيمس كالستروم. وقد صعد نجمه يوم كان رئيس فريق التكنولوجيا في المكتب، لنجاحه في عملية التنصّت التي أوقعت جون جوتي. ووصفه بعض الناس بأنّه نسخة مكتب التحقيقات الفيدرالي من كيو Q، الساحر الذي عرفناه يأتي بالابتكارات والاختراعات الخارقة في أفلام جيمس بوند. وكان أسلوبه في العرض الحديث المباشر والنظر في عيني مستمعيه، وتوجيه انتقاداته بشكل شخصي. فيسألك هل أنت متزوج؟ هل لديك طفل؟ ثم يندفع بجرأة إِلىٰ عرض سيناريو يصور فيه قيام أحدهم باختطاف أحد أولادك، واحتجازه في قلعة في منطقة البرونكس. وتذهب الظنون بالمكتب أن ولدك محتجز هناك؛ فيحصلون على مذكرة تفتيش للعثور عليه. لكن الأوغاد قد شيَّدوا القلعة من معدن جديد ليمنعوا اختراقها. لذلك يقف الرجال المكلّفين بإنقاذ ولدك عاجزين، عن دخول القلعة المنيعة. ويا له من كابوس رهيب: المختطفون، ومعهم رهينتهم الثمينة، يراقبونك ورجال الحكومة وأنتم تحاولون الدخول ويضحكون عليكم.

سوف يقول كالستروم بلهجته النيويوركية: «إن هذا هو الأساس الذي تقوم عليه المسألة. ومن وجهة نظر حفظ النِّظام، هناك تهديد خطير ـ هذا الشخص سوف يقوم الآن ببناء هذه المنطقة المحصّنة في برونكس، لأن لديه باباً فولاذياً ضخماً، ولا شيء لدينا من أدوات اللحام، والبومرنج boomerange [سلاح أسترالي يصيب هدفه ثم يرتد عائداً إِلىٰ صاحبه هـ. م] يفتح لنا الطريق

إلىٰ داخل ذلك المكان. إننا بالتأكيد، نريد أن نمتلك تلك الأبواب الفولاذية الجديدة، لحماية مصارفنا، وأسرار التجارة الأمريكية، وحقوق الملكية، والتكنولوجيا. ولكن هل نرغب في طريقة رقمية فائقة السرعة، حيث يستطيع المجرمون الكبار العمل، دون أن يتأثّروا بالأوامر القضائية، أَو يتضايقوا منها؟ إذا كنا لا نرغب في ذلك، عندئذ يجب علينا أن نتطلع إِلىٰ «المقراض».

أضحى كالستروم ومعه كل من بيكر، وبروكس، ومك كونيل، وجون دويتش رجل وكالة المخابرات المركزية (سي آي إيه)، جزءاً من فريق وديعة المفتاح يعرضون ظاهرياً للإدارة ما لديها من بدائل، لكنَّهم كانوا يوجهونها حقاً، بيد واحدة على مؤخرة عنقها الديمقراطية، نحو القبول المحتوم بالمقراض. كان ثمة حليف أتت به الرياح على نحو غير متوقّع هو رون براون وزير التجارة؛ ففي أول عرض حضره، ذكر براون أنّه أمضى خدمته الإلزامية في دائرة التنصّت بوكالة الأَمن القومي، وكان مدركاً تماماً ما تتمتّع به استخبارات الإشارة من أهمية حيوية. وفي هذه المرحلة أصبحت جلسات الاطلاع لا تقتصر على جماعة الأمن القومي بل اتسعت لتضم المستشارين العلميين لدى كلينتون وجور مثل مايك نيلسون الذي يعمل في مكتب السياسة العلمية والتكنولوجيا، مهووسون بالمعلوماتية، متفهمون منسجمون مع قضايا مثل الحرية الشخصيَّة وحاجة الصناعة إِلىٰ أنظمة مأمونة. (حصل نيلسون على تصريحه الرسمي السرِّي للغاية بسرعة البرق في غضون ثلاثة أسابيع). وفي عرض لمكتب التحقيقات الفيدرالي في 26 كانون الثاني/ يناير، فسَّر كالستروم الكثير من النقاط الدقيقة في المشروع، لكن المدير المسؤول عن برامج الاستخبارات لدى جور، جورج تنيت طرح المزيد من الأسئلة حول منهج المقراض، مثل من سيكونون الوكلاء لوديعة المفتاح؟ كيف ستتم معالجة الجوانب الدولية؟ وتضمّنت مذكرة مسهبة وضعها سيشون في 9 شباط/ فبراير ملخصاً مفصلاً للخطة، والآثار الخطيرة التي ستنجم، إن لم يتم الشروع في عمل ما.

وهكذا، لم يكن قد مضى شهر على تولي إدارة كلينتون، حتى اشتد الضغط للإسراع في تنفيذ المقراض. وكان مفترضاً، أن تشحن إيه تي أند تي عشرة آلاف جهاز هاتف، مزودة بمعيار تشفير البيانات، بحلول الأول من نيسان/ أبريل ما لم يمنع ذلك إجراء ما. لكن بحلول ذلك الوقت، كان فريق الشّيفرة لدى الإدارة ـ المؤلّف من أعضاء مجلس الأَمن القومي، وخبراء في الإنترنيت ـ قد انتقلوا تدريجياً من صنع القرار إِلىٰ تنفيذه. كانت تلك المبادرة الكبيرة الأولى لهم، وكانوا يرغبون بالقيام بها سريعاً: وظلت الكلمة «إنهاء» تبرز في مراسلاتهم. في مذكرة داخلية من النوع المعهود، مؤرخة في 5 آذار/ مارس، وجّهها جورج تنيت إِلىٰ ليون فيورث، مستشار جور لشؤون الأَمن القومي وزميله ويليام وايز: تصدرت الرأسية عبارة «النجدة، النجدة، النجدة». ثم «إن الحاجة ماسّة لأن يمنحنا نائب الرئيس بعضاً من وقت، لعقد اجتماع مع مدراء وكالة الأَمن القومي السابقين والحاليين. حول مسألة التشفير. «أظن أنني أعلم ما يرغب نائب الرئيس في سماعه من حديث مك كونيل وستوديمان»، وأنهى تنيت مذكرته بخاتمة غريبة: «رعاكم الله جميعاً!».

تواصلت الاجتماعات طوال شهر آذار/ مارس، وفي غضون ذلك، كانت جماعات الصناعة والحريات المدنية تمارس ضغوطاً على القادمين الجدد، وهم ما يزالون يأملون من الإدارة الجديدة القبول بإجراء إصلاح كبير في موضوع الشّيفرة. وصرخ أحدهم بجماعة جور قائلاً: «إنّكم تعرقلون التجارة الإِلكترونية، إنّكم تعرّضون أمن الشبكات للخطر، وإِلىٰ جانب ذلك، فإنّها خرجت جميعها عن نطاق السيطرة». ولكن جماعة كلينتون كانوا لتوهم قد انحازوا ذهنياً إِلىٰ المطلعين على بواطن الأمور في الحكومة داخل وكالة الأَمن القومي، ومكتب التحقيقات الفيدرالي، ووزارة العدل، ووكالة المخابرات المركزية. ولقد أدّت جلسات الاطلاع السرّيّة الغرض المطلوب، وعلى وجه الخصوص التحذير، بأنّه ما لم يُتخذ أي إجراء فإن «الناس سوف يُقتلون، ولقد

سُئلوا: هل أنتم على استعداد للتضحية بحياة البشر، من أَجل زيادة جزء من فاصلة عشرية في مجمل الناتج القومي؟» وكانت الخطة مؤثرة على نحو مدمِّر: فقد حُلّت المعضلة بشكل جوهري بوصفها خياراً بين مقتل آلاف من الناس وزيادة ثروة بيل جيتس بنسبة عشرة بالمئة. ويقول مسؤول في الإِدارة: «كان هذا قراراً سهلاً إِلىٰ حدّ بعيد».

ومؤدى ذلك أنّه لم يكن ثمة ارتياب داخل البيت الأبيض. فقد كان السؤال الكبير الذي طرحه مساعدو كلينتون على أنفسهم: «لماذا يرغب أي شخص بالمقراض؟» (ففي النهاية، «كان» يفترض بالخطة أن تكون طوعية). وكان ثمة مشكلة أخرى، بعد، وهي المطلب بأن تكون خوارزمية الوثاب محجوبة. وكان من المحتم أن سريتها سوف تقود النقاد إِلىٰ القول بأن المشروع كان بمثابة حصان طروادة لإِدخال شيفرة فيها عيوب إِلىٰ البنية التحتية. لكن وكالة الأَمن القومي ما كانت لتتزحزح عن موقفها من السرِّيَّة.

أخيراً كان ثمة مشكلة، كيف سيعمل مشروع وديعة المفتاح فيما وراء البحار؟ فإِذا لم يكن الحل التشفيري عالمياً، فإِنّه سيكون عديم الفائدة. وإِذا لم تحظ منتجات الولايات المتّحدة مع خطة الوديعة بثقة المشترين في الخارج، فإِنَّهم سوف يعرضون عنها ويلتفتون لشراء احتياجاتهم من المصنّعين في سويسرا أَو ألمانيا أَو حتى روسيا. ثم كيف بمقدورك أن تعالج وديعة المفتاح في البلدان الأخرى؟ هل يجب على الولايات المتّحدة أن تسمح لدول تفتقر لحرية التعبير عن الرأي مثل سنغافورة والصين بالوصول إِلىٰ المفاتيح المخزّنة؟ وهل ستكون فرنسا ومصر واليابان ودول أخرى سعيدة بالسماح لمواطنيها باستخدام منتجات تتيح لأشباح في الولايات المتّحدة حل شيفرة المكالمات، بينما لا تستطيع ذلك وكالات الاستخبارات وأَجهزة حفظ النِّظام في تلك البلدان؟ إن هذه الأسئلة لم تكن لتجد لها إجابة بسبب من أن المخططين للمقراض لم يوجدوا أبداً حلاً لآثاره العالمية ـ وتلك نتيجة أخرى تأتت مع الإِسراع بطرح المقراض.

إن هذه الاعتراضات كلها لم تكن كافية لإغراق الخطة. ففي السادسة من مساء 31 آذار/ مارس 1993، وفي غرفة إِدارة الأزمات بالبيت الأبيض، قام نائب الرئيس جور بمراجعة للتوجهات المقترحة في اجتماع ضم المجموعة بأكملها من قادة أَجهزة حفظ النِّظام والاستخبارات و الأَمن القومي. وبعيد ذلك، عرض للرئيس توصيته. فوافق بيل كلينتون.

وجاء الأمر بتنفيذ المقراض.

منذ تلك اللحظة، تحوّلت العمليَّة إِلىٰ ما أَطلق عليه أحد المساهمين فيها اسم «تسويق على طريقة البيت الأبيض». ووضعت مسودات البيانات الصحفية. وأخذ مايك نيلسون بكتابة توضيح للاقتراح بشكل سؤال وجواب. ومن ثم عشية الإعلان ذاته، أطلع البيت الأبيض مسبقاً عدداً من ممثلي الكونغرس والصناعة، وجماعات الحريات المدنية على الموضوع، ولم يكن ذلك بقصد الحصول على تغذية راجعة، بقدر ما كان لمنع توجيه التهم التي كان جماعة كلينتون قد تعاموا عنها مع التحوّل المفاجئ في مجرى المشروع.

ومع ذلك، لم يتوقع أحد في البيت الأَبيض، قيام ضجة حول المقراض. لكن كلينت بروكس رأى مشكلة قادمة، كانت هذه المسألة عرضة لاحتمال أن تتسرّب إِلىٰ خارج وكالة الأَمن القومي، لتجعل من المتعاطفين المحتملين أعداء حقيقيين. وذات مرة، أثناء تنقّله بالسيارة مع ستوبيكر بين فورت ميد والبيت الأَبيض قال له متذمراً: «إنهم قاصرون عن إدراك المسألة». وفي أحد الاجتماعات، تساءل: «من الذي سيعالج هذا الموضوع في برنامج لاري كينج الذي يبثّ على الهواء مباشرة؟» ولقد تجاهل الحضور هذا السؤال. فكرَّر من جديد بعد بضع دقائق. فأخبره مسؤول كبير في الإِدارة بصرامة: «يا كلينت، إننا نقدّر موهبة الدعابة عندك. لكن هذا أمر جدي فعلاً. عليك بمعالجة الجانب التقني من الموضوع، ونحن سنعالج الجانب السياسي». (بعد بضعة أشهر عندما ظهر آل جور في برنامج لاري كينج، ليتحدّث عن طريق المعلومات

السريعة، كان أول سؤال وجّه إليه يتمحور حول. . . رقاقة المقراض).

مضت جلسات الإطلاع مع الكونغرس، وأرباب الصناعة على نحو كان متوقعاً تقريباً: فقد استقبل الاقتراح بحذر بل حتى بالشكّ لكن دون أن يصرف النظر عنه. وتذمّر أحد المستشارين في الكونغرس بأنّه عندما جرى تحدي جماعة كلينتون ردّوا بموقف هجومي. فقد تساءلوا: «هل ترغبون في أن تكونوا مسؤولين عن الخاطفين؟» فتهاوى المشرعون. ولم تكن الجلسات التي عُقدت مع جماعة الحريات المدنية بعيدة كل البُعد عن الودّ والمجاملة. ولقد حضر جون بيري بارلو من مؤسَّسة الآفاق الإِلكترونية إحدى الجلسات الاطلاعية المفاجئة ولم يستطع أن يصدّق ما يسمع. إذ شعر بأن أصدقاءه الجدد في البيت الأَبيض كانوا يشربون ما تقدمه لهم وكالة الأَمن القومي. وما أزعجه بشكل خاص ذكر مايك نيلسون للمعلومات السرِّيَّة التي بلغته ولم تكن قد بلغت بارلو. قال نيلسون: «لو كان بإمكاني أن أخبرك بما أعلم، لشاطرتني الشعور ذاته». وأسرّ إليه بأن الآلاف يمكن أن يلقوا حتفهم. فشعر بارلو أنّه كان يسمع الموسيقى الزائفة ذاتها التي كان يعزفها مثيرو الحرب الفييتنامية. وأن ما يعنيه المقراض حقاً، كان خطة سوف «تبدأ عمليَّة قد تشكل نهاية الحرية في أمريكا».

وقام كلينت بروكس، ببذل جهود كبيرة، ليفهم الخبراء في الخارج المعلومات الضروريَّة ليشرحوا للجمهور الطبيعة غير الخطرة للنظام. وفي الليلة التي سبقت الإعلان، قام بروكس بالمجازفة بقيادة سيارته تحت وابل من المطر ليطلع دوروثي دينينج، أستاذة علم الكومبيوتر في جامعة جورجتاون، ويعرض عليها خياره الأول لعقد ندوة لدراسة خوارزمية الوثاب السرِّيَّة. وكان ذلك خياراً ملهماً. ذلك أن دينينج كانت خبيرة في الشّيفرة وأمن الكومبيوتر لكن سلوكها كان من الرقة مثلما كانت عليه بيتي كروكر. (وصف كاتب الخيال العلمي بروس ستيرلينج ذات مرة المرأة الدقيقة الحجم هذه بأنَّها «أشبه براهبة حاجة خلف زجاج من الرصاص») وكانت في ذلك الحين معروفة بدعمها لضبط

الكريبتوجرافيا، وبمحض الصدفة، وبالتزامن مع زيارة بروكس، كانت لتوها قد خبرت وضعاً مزعجاً عجزت فيه عن فتح خزانتها بعد سباحتها في مسبح الجامعة المغلق؛ ولم ينقذها سوى رجال الصيانة، ذوو الخبرة والقدرة ومعهم القاطعات المتينة (المرادف لعملاء الوديعة!) من خطر التعرّض لطقس [بارد] تبلغ درجة حرارته أربعين درجة [فهرنهايت] في ملابس سباحة مبلّلة. ولذلك فإنَّها لم تكن على استعداد للدفاع عن وديعة المفتاح فحسب، بل إنها أصبحت تشعر بأنَّه كان قدرها.

في 16 نيسان/ أبريل، كشف الرئيس كلينتون النقاب عن المبادرة الجديدة. وفي إعلان سكرتيره الصحفي عن الخطة، عرضت القضية للجمهور على أنَّها حل وسط بين أمرين أحلاهما مر، مثلما عرض الوضع للإدارة من وجهة نظر وكالة الأَمن القومي إِلىٰ حد بعيد. وبالنظر إِلىٰ الوضع عبر تلك المصفاة، تم اعتبار رقاقة المقراض هبة من الله:

إن الرقاقة خطوة هامَّة في مواجهة مشكلة سيف التشفير ذي الحدين: فالتشفير يفيد في الحفاظ على سرِّيَّة الأفراد والصناعة، لكنه بإمكانه أيضاً حجب المجرمين والإرهابيين عن الأنظار. إننا بحاجة إِلىٰ «رقاقة المقراض» وطُرق أخرى تتيح للمواطنين الملتزمين بالقانون بلوغ ما يحتاجون إليه من التشفير وتحول دون استخدام المجرمين له، لإخفاء أنشطتهم غير القانونية سواء بسواء.

إن الإعلان الفعلي عن المقراض لم يجعل منه معياراً، لكنَّه أكَّد التزام الحكومة بشراء الآلاف من أَجهزة شركة إيه تي أند تي التي وضعت رقاقة المقراض داخلها لتزود بها دوائرها. وكان الأمل أن يؤدي تبني الحكومة للمقراض وتزكيته أن يحدثا تحولاً في السوق مما يجعل المقراض يشيع وينتشر، وإن ظل اختياره معياراً طوعياً. أما التوصية النهائية فستأتي بعد تلقي كلينتون نتائج مراجعة واسعة النطاق على مستوى رفيع لسياسة الشّيفرة التي

ستعتمدها الولايات المتّحدة، بعد تفحص مبادرة الوديعة بعناية وتقوم قوانين التصدير.

وبذلك الإعلان، شعر بيل كلينتون وجماعته بأنّهم قد قاموا بخطوة كبيرة نحو تفادي ما بدا وكأنّه تصادم ينذر بكارثة في عالم الشّيفرة، تصادم بدا مقدّراً سلفاً منذ اليوم الذي اكتشف فيه هويت ديفي طريقة تقسيم مفتاح الشّيفرة. والواقع أن رقاقة المقراض اعتبرت بحقّ نقطة التحوّل في المعركة، لكن ليس بالطريقة التي كانت تريدها إدارة كلينتون على الإطلاق. فبالترويج للمقراض باعتباره سفينة القيادة لمفتاح الوديعة، ارتكبت الحكومة خطأ فادحاً. فعوضاً عن التدرج في مناقشة موضوع التشفير أصبحت فضائل هذا المشروع ـ ومثالبه ـ هي ساحة القتال الرئيسة في معركة حامية الوطيس حول التشفير. كان المقراض ذاته هو القضية، وكان المقراض كما تم اقتراحه عرضة للانتقاد. وقد رأى مهندسه كلينت بروكس، أكثر من أي شخص آخر، ما كان يجري، لكنه كان عاجزاً عن منعه.

في البداية، لم تبدو الأمور سيئة إلىٰ حد كبير. ومن الموقع الممتاز للبيت الأبيض وفورت ميد، بدا أن أي اهتمام شعبي ضئيل نسبياً حظيت به رقاقة المقراض، كان متوازناً بكل معنى الكلمة. وقد حدّدت مقالة النيويورك تايمز، المنشورة يوم الإعلان، لهجة معقولة في تناول الموضوع من مقدمتها، إذ قالت أن إدارة كلينتون «على وشك إعلان خطة لصون السرّيّة في وسائل الاتّصال الإلكترونية... فيما تتضمن كذلك حق الحكومة بالتنصّت لأسباب تتعلّق بحفظ النّظام و الأمن القومي». التوازن. وبالطبع، فإن المقالة أوردت قولاً لأحد ممثلي الوسط لصناعي: «إن الحكومة في سبيلها لأن تُخلق وحشاً».

وفي الأيام التالية، لم يكن ثمة أي استعجال لقبول الخطة، من مختلف أصحاب المصالح الذين قد يتأثّرون بها. وارتاح الفيدراليون، مع ذلك، لأنّهم

تفادوا بهذا القرار، نشوب حركة تنديد عنيفة. وأخذت الإنترنيت، تضج بمخاوف من تفشي إجراءات الدولة البوليسيَّة، ولكن من الناحية الأخرى، أعلنت دوروثي دينينج على الفور وصفاً صادراً عن فكر صاف للنظام ذاته مما اعتُبر في ذلك الحين مثالاً على أن مجتمع الشّيفرة لم يكن مناهضاً للمقراض على وجه الإطلاق. والأفضل من ذلك، أن مارتي هيلمان طلع بوصف مؤيد للخطة لم يكن متوقعاً أن يصدر عنه، وكان بروكس قد عرض له الموضوع على الهاتف عشية الإعلان. كان تفسير هيلمان للمشروع حيادياً وحذراً (مع أنّه نبّه حقاًإِلىٰ ضرورة أن يرافق هذا ضوابط للعمليَّة القانونية تؤدي إِلىٰ استرداد المفتاح)، وقامت الشبكة ذات النفوذ التي يديرها ديڤيد فاربير بإدراج اسمه ضمن قائمة «الشخصيات المثيرة للاهتمام»، ليكون في عداد من يتلقون رسائلها البريديَّة.

في 20 نيسان/ أبريل وضع كلينت بروكس، مذكرة تعكس تفاؤله كتب فيها: «إن ردود الفعل التي تردني من الأكاديميين والصناعيين تفيد بأنَّها قد تصادف النجاح». كذلك كان هؤلاء الأشخاص يقولون له بأن الحكومة ربما لم تعين عدداً كافياً من الأرقام في حقول تعريف الرقاقة لتعالج جميع رقاقات المقراض التي ستدخل في الاستعمال. إن مئة مليون لن تكون كافية!

لكن ذلك النجاح الأولي كان وهماً، وأشبه بفريق بيسبول من الدرجة الثانية احتل المرتبة الأولى بعد أن صادف سلسلة من الانتصارات في شهر نيسان/ أبريل. وقد جاءت أولى الأصوات المتذمّرة الجدية من صناعات المعلومات الدقيقة. وبعد القيام بمراجعة الخطة، خلصوا إِلىٰ أن الفرصة التي أتاحتها لبناء شيفرة منيعة قابلة للتصدير في أنظمتهم قد نال منها كثيراً وجود مجال مدخل حفظ النِّظام LEAF، الذي زود متطفلي الحكومة الذين لديهم الترخيص بالمفاتيح. وكانت الغاية من تصدير الشّيفرة، بعد كل شيء، خدمة الزبائن فيما وراء البحار. لكن ما هي الشركات الأجنبيَّة التي ترغب في شراء

نظام أمني، مفاتيحه مودعة في خزائن حكومة الولايات المتّحدة؟ وانضم كبار رجال الأعمال، إِلىٰ جماعة الحريات المدنية المرتابين أصلاً، والذين رفدتهم مجموعة الإنترنيت الأساسية بالطاقة. ثم أخذوا جميعاً قضيتهم إِلىٰ وسائل الإعلام. ومع أن بناء رد الفعل قد استغرق بضعة أشهر، فإن التغطية التي نالها المقراض في وسائل الإعلام، تجاوزت كل دعاية جماهيرية نالها سابقاً أي تطور في علم الشّيفرة.

كان بعض هذه التغطية إيجابياً. وكان مبتكرو الوديعة يعتقدون ضمناً، طوال الوقت الذي كانت فيه الحكومة تخطط لمبادرة الوديعة، بأن قلّة ضئيلة منعزلة فقط هي التي ستشكك في دوافعهم. ونظروا إِلىٰ الترويج للمقراض على أنه عمليّة ستحمل إِلىٰ العقلاء قدراً من الهموم، وأن الحكومة سوف تستجيب لها، ومن الهموم الرئيسة كما حسبوا، الخطر بأن الجانب التقني من مشروع الوديعة، سوف يعرّض أمن التشفير ذاته للخطر، مما ييسّر على المحتالين والجواسيس من دول أخرى أمر فكّ الشّيفرة، وهناك، بعد، همّ آخر هو احتمال أن تكون تسهيلات مفتاح الوديعة ذاتها ضعيفة، والذي لم يأخذه هذا التفكير بعين الاعتبار هو الأساس الذي بني عليه هذا المشروع من حيث أنه وسيلة الحكومة لنقر مفتاح «فك التشفير» لأغراضها الخاصة، وقد وجده معظم الناس كريهاً مقرفاً. كل ما كان على الخصوم القيام به هو إجراء عمليّة مقارنة بسيطة، ماذا لو أنّك كنت مضطراً لأن تترك نسخة مفتاح باب بيتك في مخفر الشرطة؟ فحتى الساذج من الناس الذي لا يعرف الفرق بين التشفير وتمرير الكرة سوف يتحوّل إِلىٰ مناهض للمقراض. وقد بيّن جيري بيرمان من مؤسّسة الآفاق الإِلكترونية بأن «الفكرة القائلة بأن الحكومة تمتلك المفاتيح لجميع الأقفال، حتى قبل أن يتهم أحد بارتكاب جريمة، قول لا يفهمه الجمهور، إن هذه ليست أمريكا».

ولم يكن الآخرون بحاجة إِلىٰ عقد مقارنة كهذه. ذلك أن أحد الأسباب

الرئيسة وراء رغبة الكثير من الناس في استخدام الشّيفرة، إبقاء المعلومات بعيداً عن متناول الحكومة ذاتها. وليس لكونهم قد انتهكوا القانون بالضرورة، بل إن الأمر بكل بساطة أنهم لا يمحضون الحكومة ثقتهم. فالبيروقراطيون الذين أعدوا الخطة كان يفصلهم جيل عن ووترجيت، ولكن أي شخص كان موجوداً في السبعينات، ربما كان يعرف الوضع بصورة أفضل.

كان مدير وكالة الأَمن القومي السابق بوبي إنمان، مثلاً، قد اطلع في وقت مبكر على رقاقة المقراض وأدرك على الفور ألاّ أمل لها بالنجاح. فمن تراه الذي أراد أن يعطي الحكومة سبيلاً مباشراً لاستقاء أخبارك؟ وقد فهم زعران الشّيفرة ذلك، وبدأوا على الفور بشنّ حرب غير تقليديَّة تستهدف وسائل الإعلام والسكّان عموماً لحملهم على مناصرتهم في حربهم هذه ضد رقاقة المقراض. وفي الاجتماع الشهري، ألحّ إيريك هيوز على أن يتضمّن جدول الأعمال كل الأعمال المحتملة بدءاً من توزيع مواد إعلامية لكسب تأييد جماعات الصحفيين إِلىٰ الدعوة إِلىٰ إجراء تعديل في الدستور ينحو إِلىٰ تأييد الشيفرة. واقترح تيم ماي القيام بعمل تخريبي فعّال للمقراض، أو مقاطعة شركة إيه تي أند تي. وقد أنجزوا حقاً مزحة مؤثّرة، بتوزيع أشكال صغيرة لتلصق على الملابس. وقد صمّمت بحيث تشابه البرمجية الشهيرة إنتل في الداخل، الموضوعة بلغة لوجو، وتقرأ عليه عبارة «الأخ الكبير في الداخل». وهذه العبارة أجملت كل ما يمكن أن يقال تقريباً. (هدّدت إنتل سريعاً بمقاضاتهم لانتهاكم علامتها التجارية، فأوقف زعران الشّيفرة توزيع اللصاقات).

جاءت المعارضة من كافة الجهات. ووجد مناهضو المقراض أنفسهم يتفقون مع راش ليمبو الذي هاجم المقراض في برنامجه الإذاعي. كذلك أعجب هيبيو الديجيتال بالعمود الذي كتبه وليام سافاير بعنوان «أغرقوا رقاقة المقراض» حيث أشار إِلىٰ أن اسم الحل المقراض Clipper قد تم اختياره بعناية، إذ أنّه يقص Clips أجنحة الحرية الفردية».

كثيراً ما كان تيم ماي يعرض لنظرية تقول، أن للأمريكيين عقلين عندما يتعلَّق الأمر بالسرِّيَّة. أحدهما يؤثر المصلحة العامة، وهو مناهض للشيفرة في الجوهر: «ماذا لديك لتخفيه؟» أما الآخر فيعبر عن الأخلاق الفردية كما يجسِّدها ميثاق الحقوق، وهو مؤيد للسرِّيَّة: «لا شأن لكم بما يخص سواكم». ولا بد لأي سياسة ناجحة من السير في طريق وسط بين هذين الاتجاهين المتعارضين. لكن المقراض، بإِصراره على ألا يخفي شيئاً عن الحكومة، لم يحقِّق التوازن المنشود. وما أن بدأ الناس يطلقون عليها اسم رقاقة الأخ الكبير، حتى انتهت اللعبة.

بذلت الحكومة قصارى جهدها للدفاع عن المشروع. وقام ستيورات بيكر بعرض الأمر لرجالات الصناعة، بما في ذلك مؤيد الشيفرة بيل جيتس، ولكن دون جدوى. كذلك دخل إِلىٰ عرين الأسد، متحدثاً في مناسبات أقيمت تأييداً للشيفرة مثل مؤتمر «الكومبيوتر والحرية والسرِّيَّة» حيث قلَّل من شأن القوى المناهضة للمقراض في وجوههم، معتبراً ما يقومون به: «انتقام أناس لم يستطيعوا حضور احتفالات وود ستوك لانشغالهم بواجبات مدرسيَّة تثقل كاهلهم». وعمد إِلىٰ توبيخهم والسخرية منهم، بقوله: «لو أنكم تعلمون ما أعلم». وجادلهم إن نظرتكم إِلىٰ السرِّيَّة تعكس رؤية للعالم ساذجة وميئوس منها. ومضى بيكر محذِّراً: «إننا بإصرارنا على حق المطالبة بسرِّيَّة تتجاوز نطاق النِّظام الاجتماعي، ونُخلق عالماً يزدهر فيه [المحتالون والإرهابيون]، وهم قادرون على القيام غداً بما هو أكثر مما يستطيعون القيام به اليوم».

لكن لم تكن جميع الأخبار سيئة بالنسبة للحكومة. ففي صيف 1993، اعتبرت خوارزمية الوثاب منيعة، في نظر فريق من «الخبراء المستقلين» بقيادة دوروثي دينينج ويضم كلاً من والت تكمان (الذي قاد فريق معيار تشفير البيانات لدى شركة آي بي إم) وإِيرني بريكيل (الذي فاز بجائزة الألف دولار، لقيامه بتفكيك شيفرة الحقيبة المتعددة التكرار لميركل). وأصبحت دينينج شديدة

الضراوة في دفاعها عن الحكومة، مبينة بوضوح موقفاً يثبت الأخطار الناجمة عن فوضى التشفير، حتى أن النقّاد كانوا يطلقون عليها اسم «القراضة الحسناء» وقد جعلتها نزاهتها أشد تأثيراً في المنتديات العامّة من الفريق التقني للإدارة المنهك والذي أخذ ظهوره في المؤتمرات ذات الصلة بالإنترنيت يلقى من الحضور ما تلقاه عملية جراحية في الأسنان من ابتهاج وترحيب. فمن تراه يلومهم والأسئلة تنهال عليهم سؤالاً بعد سؤال وكلها تحفر في الحقيقة بأن أنصارهم الطبيعيين من الراسخين في التكنولوجيا كانوا ينظرون إليهم على أنّهم أشبه بأصحاب القمصان السمراء؟ [فاشيون. هـ. م] وأصبح مايك نيلسون من البيت الأَبيض يشير إِلىٰ الشّيفرة بوصفها «بوسنة الاتّصالات عن بُعد».

وما زال المقراض كما يبدو شيئاً ملعوناً. فعند كل منعطف كانت تبرز مشكلة جديدة على نحو غير متوقع. مثلاً، بعيد الإعلان عن الخطة اتصل بالحكومة أستاذ في معهد ماساتشوسيتس يدعى سيلفيو ميكالي. وكان ميكالي الذي عمل في مجموعة الكريبتوجرافيا والرياضيات في المعهد (بقيادة رون رايفست)، قد ابتكر بضعة بروتوكولات رياضية، أطلق عليها اسم «أَنظمة شيفرة عادلة» بدت مماثلة لمشروع وديعة المفتاح الحكومي. وكان قد نشر بحثاً حولها عام 1992 وحصل على براءة اختراع عنها. فدفعت الحكومة لميكالي مليون دولار لقاء إجازة استخدام اختراعه.

كما ثبت أن اسم الرقاقة كان مشكلة أيضاً. وقد كتب بروكس في مذكرة وضعها في وقت مبكر من عام 1992، «كان المقراض الاسم الذي استترنا به في عمليات وكالة الأَمن القومي العادية. وحاولت أن أحمل الناس على عدم استخدامه خارج الوكالة، لكن صناع السياسة ومستشاريهم وجدوا أن من الملائم جداً استخدامه إِلىٰ حدّ أنّه صار ملازماً له». ومن المؤسف أن شركة تدعى انترجراف، كانت تبيع في ذلك الحين معالجاً مصغراً أطلقت عليه اسم «المقراض»، فاضطرت حكومة الولايات المتّحدة أن تدفع لها مبلغاً كبيراً لقاء

استخدام هذا الاسم، الذي كان على وشك أن يصبح ما يطلق عليه المسوقون اسم مشؤوم.

أما المشكلات الأخرى فكانت محض تقنية. ومن ذلك ما صادف مصنِّع الرقاقات مايكو ترونكس، وكان مقاولاً حكومياً وتجارياً غير معتاد على طلبات السوق الاستهلاكية، ولم تكن الرقاقات مبنية لتتزود بمعدلات مرتفعة من البيانات. وفي إسراعها لإدخال المقراض على هواتف إيه تي أند تي، كانت وكالة الأَمن القومي قد ابتكرت منتجاً يمكن أن يلائم تكنولوجيا الاتِّصالات لعام 1993 لكنه كان غير كفء على نحو يرثى له لأن يكون مناسباً للسرعة الكبيرة لتدفق المعلومات في المستقبل القريب الذي لا بد آت ربما بعد عامين أَو نحو ذلك. وبكلمات أخرى، كما لاحظ النقاد بسخرية مريرة، بحلول الوقت الذي يستغرق في شركة ناجحة الأشهر الخمسة عشر إِلىٰ الثمانية عشر لبناء مُنتَج حول المقراض سيكون العتاد قد تجاوزه الزمن.

«هل أحب أحدكم المقراض؟» كان قد طلب من المؤسَّسة القومية للمعايير والتكنولوجيا، معرفة تعليق الجمهور على الخطة، كجزء من العملية، فكان أن وجهت هذا السؤال. وقد استجاب ثلاثمئة وعشرون فرداً ومنظمة اثنتان منها فقط قابلت فكرة المقراض بالرضا. وهذا ما جعل لين مكنولتي المسؤول في المؤسَّسة القومية للمعايير والتكنولوجيا، يسلم بأن «ليس هذا بالتزكية الطيبة لبلاء مجيد».

لكن جماعة كلينتون لم يتزحزحوا عن موقفهم. ففي 4 شباط/ فبراير من عام 1994، صادق الرئيس رسمياً على المقراض ـ المعروف باسم معيار وديعة التشفير ـ بوصفه معيار معالجة المعلومات الفيدرالية. وسوف تشرع الحكومة على الفور في شراء هواتف إيه تي أند تي المجهزة بالمقراض لاستخدامها الخاص، وإيداع المفاتيح في المؤسَّسة القومية للمعايير والتكنولوجيا ووزارة المالية. (على الرغم من أن التكنولوجيا لم تكن متوفرة فعلاً، بعد، للقيام بفك

الشيفرة للمفاتيح المسترجعة من تسهيلات الوديعة غير الموجودة حتى الآن).

كتب تيم ماي: «إن إعلان الحرب علينا وشيك، فقد أظهر جماعة كلينتون وجور أنفسهم، بمظهر المؤيدين المفعمين حماسة للأخ الكبير».

وفي مجلس الشيوخ أقسم باتريك ليهي مع آخرين سواه، على محاربة المقراض، وألح على أنَّه دون موافقة الكونجرس لا يمكن تمويل المشروع (كلفة وضع البرنامج تبلغ 14 مليون دولار، إضافة إِلىٰ 16 مليون دولار سنوياً مخصصة لتسهيلات الوديعة). وفي أيار/ مايو 1994 عقد السيناتور ليهي جلسة استماع. وفي ظهور علني نادر عرض كلينت بروكس ومايك مك كونيل للمشهد، من وجهة نظر من وراء السياج الثلاثي، مهنئاً الإدارة لاتخاذها الطريق الصحيح. وخلص مك كونيل إِلىٰ القول: «هنالك، بلا ريب، مسائل ينبغي تسويتها، لكنني على ثقة من أننا سوف نتخلّص من الشوائب وتستقيم الأمور».

ثم أظهرت مجموعة من المناوئين، أن تلك «الشوائب» بحجم حوض نهر كولورادو تقريباً.

وكان من بين الأسئلة العسيرة التي وجهوها: «من الذي سوف يقبل على استخدام المقراض، في حين أن هناك برامج جاهزة مثل بي جي بي؟» وكانت استجابة الحكومة «نظرية اللص الغبي»، التي شرحها جيم كالستروم من مكتب التحقيقات الفيدرالي على أحسن وجه، والذي زعم بأنه حُمل على سماع رجال عصابات كانت خطوطهم الهاتفية مراقبة، يسخرون من كونهم يخضعون للتنصّت، ويشاركون في أحاديث فيها إدانة لهم لتورطهم في أعمال إجرامية، لمجرد أنَّهم يجدون مشقة في الخروج واستخدام هاتف للعموم. وقال: «إذا ما راج المقراض في غضون خمس سنين، ووضعه الناس في أجهزتهم، فإن نسبة عالية من المجرمين سوف يذهبون إِلىٰ راديو شاك، أَو أي مكان آخر مشابه له لشراء مفكك تشفير من نوع ما. إنهم لن يتذكّروا أنَّه في عام 1994 [ظهرت] مقالة هامة في مجلة وول ستريت جورنال [حول وديعة المفتاح]. ولربما وقعنا

في مكان ما من المطبوعة الراقية على أن المقراض شيء ذو شأن. لكن لن يكون ظاهراً لكل ناظر [بل] سوف يكون جزءاً من المشهد العام. وهذا مبتغانا».

حسن، إذن فقد يستخدمه اللصوص الأغبياء. ولكن الشهود المناهضين للحكومة لاحظوا أنه إذا ما أعرض المجرم الذكي عن المقراض، فإن الزبائن فيما وراء البحار الذين لهم أعظم الأهمية في تبنيه، سيفعلون ذلك أيضاً. فما الذي يحمل فرنسا، أَو اليابان، أَو إندونيسيا على التوقيع على خطة تجعل المفاتيح لمحادثات مواطنيها الخاصة ـ التي ربما تتضمن أسراراً تجارية لا تقدّر بثمن ـ بيد فرعين من أَجهزة حكومة الولايات المتّحدة؟

ولربما كان هويت ديفي الشاهد الأكثر إقناعاً. وقد شهد ليس بوصفه أحد مبتكري المفتاح العام وحسب، بل بوصفه أيضاً ممثلاً لإحدى جماعات الضغط المناوئة للمقراض، جماعة العمل من أجل الأمن والسرِّيَّة الرقمية. حاول ديفي أن يضع المسألة في منظور تاريخي. فالحكومات كانت معنية على نحو مماثل بالثورات السابقة في مجال الاتِّصالات، مثل الكيبل الممتد عبر الأطلسي وشيوع الراديو. وبالرغم من المخاوف التي كانت تنتاب الحكومات من أن تفقد سيادتها، فقد ثبت في النهاية أن هذه التطورات كانت ذات فائدة عظيمة لها. والآن يُرجَّح أن تزيد الاتِّصالات بالكومبيوتر إجمالاً في قوة الدولة. لكن الولايات المتحدة بدت كارهة لأن يكون لمواطنيها أياً من تلك القوة. وفي حين أن الحكومة تدعي الرغبة في الاحتفاظ بقدرتها على التنصت وحسب، فإن الحقيقة أنَّه في عهد الآباء المؤسسين، كان من السهل الحصول على السرية، بمجرد الابتعاد عن مدى سمع الآخرين. وقال ديفي: «يبدو أن حق المجتمعين في اتخاذ التدابير لضمان سرِّيَّة الحديث كان أمراً يكاد لا يقبل الشك، بالرغم من أن حق سرِّيَّة الحديث قد يُساء استعماله فيكون في خدمة الجريمة». واليوم، يتصل الناس ببعضهم، بطُرق إلكترونية، إلىٰ حد بعيد، تراوح بين الهاتف

والكومبيوتر. فهل يمكن أن يكون للحكومة، الحق في منع السرِّيَّة في هذه المحادثات؟ وأخبر ديڤي أعضاء مجلس الشيوخ: «إن شرعية القوانين في المجتمع الديمقراطي تنشأ عن السيرورة الديمقراطية. وما لم يكن الناس أحراراً في مناقشة الآراء المطروحة حول القضايا ـ والسرِّيَّة مكون أساسي للعديد من هذه المناقشات ـ لا يمكن لتلك العمليَّة أن تتحقَّق».

بعيد انتهاء جلسات الاستماع في مجلس الشيوخ، تعرض المقراض لضربة قد تكون الأسوأ بين جميع الضربات التي تلقَّاها. ولم تأت كخطبة مسهبة عنيفة في الكونجرس، أَو هجوماً شنّه أحد ممثلي الصناعة، أَو مقالة غير رسمية من أحد زعران الشّيفرة، بل كانت نتيجة لتجربة علمية أجراها عالم باحث مغمور يدعى ماثيو بليز. وكان ما فعله هو أنَّه جعل رقاقة المقراض، تبدو غبية.

كان بليز من أبناء نيويورك، وباحث جريء في العلوم الكلاسيكية، وقد انقطع عن الدراسة في إحدى المدارس الإعدادية الخاصَّة، وعمل حيناً ممرضاً (أول شخص توظّفه مصلحة الإسعاف الطبي للمدينة بدون رخصة قيادة سيارة)، ثم انتقل إِلىٰ الدراسة الجامعية، وحصل على إجازة في علمين متعارضين في ظاهرهما: الكومبيوتر والعلوم السياسيَّة، وأثناء قيامه بالدراسات العليا في جامعة كولومبيا، بدأ يفكر جدياً بالشّيفرة. وخلال حديث له مع أحد زملائه في المكتب، ويدعى ستيوارت هابير، الذي كان قد ابتكر طريقة لاستخدام المفتاح العام لتأريخ الوثائق رقمياً (مقدماً مرادفاً إِلكترونياً للعادة القديمة بختم الرسالة بخاتم البريد لتحديد تاريخها)، أدرك بليز أن الشّيفرة كانت طريقة لمعالجة مشكلات هامة في الرياضيات ورافعة عمليَّة لتغيير المجتمع على حد سواء. وكان بليز كذلك شديد الإِيمان بحق الإِنسان بالسرِّيَّة.

بعد انتقاله إِلىٰ جامعة برنستون، وحصوله على الدكتوراه، مضى ليعمل مع مجموعة تشفير صغيرة في مخبر بل للبحوث التابع لشركة إيه تي أند تي.

وبدأ بليز العمل في مجالات تشفير أخرى، ما عدا الخوارزميات. وكانت مجموعته معنية بالبحث الأساسي، أكثر من مجموعة نظام الأمان، لشركة إيه تي أند تي في نورث كارولينا، التي كانت قد أنتجت جهاز تي إس دي 3600، الذي وقع الاختيار عليه ليكون جهاز الهاتف ذي المقراض. والواقع أنّه اكتشف موضوع المقراض أثناء قراءته الصحفية مثل أي شخص آخر.

لكن إدارة كلينتون، فيما هي تعد للمصادقة على معيار الوديعة في شباط/مارس 1994، أجرت سلسلة من الجلسات الإطلاعية الفنية، ضمت في عدادها مجموعة الشيفرة في مختبر بل. كذلك حضر العديد من العلماء لدى وكالة الأَمن القومي، إِلىٰ نيوجرسي للاشتراك في إحدى الجلسات الاطلاعية. ومع أنه يمكن وصف مجموعة الشّيفرة عموماً، بأنّها مناهضة لرقاقة المقراض فضلاً عن مضامين السرِّيَّة، وبوصفهم كريبتوجرافيين، فقد شعروا بالضيق من المخاطر الأمنية التي ينطوي عليها إرسال المفتاح إِلىٰ فريق ثالث، ويقول بليز: «لقد تدبرنا أن نحسن التصرف، وألاّ ندع اللقاء يهبط إِلىٰ مستوى مناقشة ما إذا كانت هذه فكرة جيدة أم لا». وفيما بعد، سأل إن كان بإمكانه أن يرسل ملخصاً لما جرى في الاجتماع عبر الإنترنيت، وكان أن التزم بليز بالوقائع في ذلك أيضاً.

وقد أثار هذا إعجاب من كانوا خلف السياج الثلاثي، الذين زين لهم الفكر على ما يظهر أنّه يمكن الاستفادة من بليز مختبر آخر من الخارج لتكنولوجيا المقراض. فتمت دعوته مع أحد زملائه إِلىٰ فورت ميد لدراسة أنموذج أولي لتيسيرا Tessera وهي النسخة التي تعتمد على البطاقة الذكية من نظام الوديعة (كان مقيضاً أن تكون تيسيرا نسخة قابلة للحمل من نظام تشفير القمة بكل محتوياته الذي كان كلينت بروكس يفضله على رقاقة المقراض المحدودة). وهناك شعر بالإثارة إذ لم يسبق له أن دخل المكان من قبل. وقد أعطي شارة الزائر المعتادة مع جهاز حسَّاس لتعقب خطواته في البناء: وحينما اصطحبه مضيفه معه، كان عليه أن يظل في مواجهة آلات التصوير الأمنية،

ويطمئن حارساً غير مرئي بأن بليز برفقته، وقال صوت يستحيل تبين صاحبه: «حسن، شكراً». حتى بين قاعة الاجتماع والحمام تكرر هذا الأمر مرتين. ويقول بليز: «لكنهم لم يتبعوني فعلاً إلىٰ الحمام»، وحين غادر علماء مختبر بل، قدمت لهم بطاقات تيسيرا ومجموعة من الكتيبات الشارحة وأباريق قوة خاصة بوكالة الأمن القومي.

شرع بليز على الفور في اختبار النِّظام، مركزاً على الجوانب المتصلة بالمقراض في الجهاز. وبخلاف فريق دوروثي دينينج، الذي ركز على الوثاب، تساءل بليز ما إذا كان ثمة طريقة، لاستخدم التشفير المنيع فعلاً بينما يجري التغلب على مقومات الوديعة. وبكلمات أخرى، هل بإمكان لص، أو إرهابي، أو شخص ما يرغب في السرِّيَّة وحسب أن يستخدم شيفرة المقراض دون أن يتم اكتشاف شخصيته؟ وقد ركَّز جهوده على دراسة مجال مدخل حفظ النِّظام. يقول: «لم أكن لأفكر حتى أن أعتبرها موطن ضعف محتمل، لكن اتضح بأن الطريقة الواضحة للتغلّب على مجال مدخل حفظ النِّظام كانت أول ما ينبغي أن يخطر ببالك».

بدأ في إجراء الاختبار، مستخدماً في ذلك قارئ بطاقة وبرنامجاً صغيراً يحاكي التنصّت عبر الأسلاك. وجرب أبسط الأشياء ـ مثل تغيير الرمز بحيث لا ترسل المعرِّف، أو إرسال رقم ما آخر محل المعرف ـ لكنها لم تنجح. إلاَّ أن الأمر استغرق قدراً من التفكير وطرقاً أكثر تعقيداً بقليل حتَّى تحقّق له النجاح. وجاء الاختراق حينما لاحظ بليز، وهو منكب على مطالعة هذه الكتيبات، بأن «ضبط المجموع» في مجال مدخل حفظ النِّظام كان مداه 16 بت فقط. (ضبط المجموع طريقة للتثبت من أن مجال مدخل حفظ النِّظام، بما في ذلك معرف الرقاقة ومفتاح الجلسة الذي قام بتشفير المحادثة، قد تم إرسالها إلىٰ المراجع فعلاً. إن العدد المناسب في ضبط المجموع أشبه بعبارة «كل شيء واضح»، التي تعني أن الأمور على ما يرام. وإذا ما كانت هنالك طريقة لتزييف مجال

مدخل حفظ النِّظام، مع ضبط مجموع صحيح، فإنك ستكون في الواقع قد ألحقت الهزيمة بنظام المقراض. إن التشفير سيعمل، لكن المتنصتين عبر الأسلاك لن يتوفر لهم مفتاح الجلسة المناسب لفكّ شيفرة المحادثة).

يقول بليز: «إن ست عشرة بت ليست عدداً كبيراً جداً في هذه الأيام، لإجراء العمليات الحسابية». وفي غضون ساعات قليلة وضع «منفاخاً لمجال مدخل حفظ النِّظام» وهو برنامج سريع يمكن أن يصدر كل تركيبة ممكنة (2^{16}) من أعداد ضبط المجموع، ثم قام بربطه بنظام الاختبار الخاص به، والحق أنه لم يكن يتوقع أن ينجح، لقد بدا سهلاً جداً. لكنَّه نجح فعلاً، في كل مرة كان يجربه فيها. وفي ما لا يزيد على اثنتين وأربعين دقيقة، كان قادراً على إرسال ضبط مجموع يخدع نظام الوديعة بأن جعله يفترض خطأً أنه كان يرسل البيانات، التي ترشد المحققين إِلىٰ المفتاح المودع، في حين أن هذه البيانات مضلّلة، ولا تقودهم إِلىٰ أي شيء. بل إن المتنصت سوف يواجه، عوضاً عن ذلك، محادثة مشفَّرة بخوارزمية الوثاب القوية الفعالة، التي تعتبرها وكالة الأَمن القومي ذاتها غير قابلة للتفكيك. (كذلك وجد طريقة تمكن شخصين متآمرين من التغلّب على مجال مدخل حفظ النِّظام بسرعة أكبر أيضاً).

وما كان يجهله بليز هو أن المدى الصغير لضبط المجموع لم يأت مصادفة بل جاء نتيجة الاستعجال في اعداد المقراض. ذلك أنه أثناء عملية التصميم المستعجلة، تشاور مهندسو وكالة الأَمن القومي، مع مختلف الخبراء الفنيين في شركات الهاتف، الذين حذَّروهم من أنَّه بعد نزول الهواتف اللاسلكية، فإن أي نظام يتطلَّب بث الكثير من البتات سوف يعتبر غير عملي. وهكذا حدّد مجال مدخل ضبط النِّظام بـ 128 بت منها، 32 بت تستخدم لتعريف الرقاقة، بينما تكرس الـ 96 بت الباقية لمفتاح التشفير وضبط المجموع. وكانت وكالة الأَمن القومي ترغب في ضبط مجموع كبير، لكن مكتب التحقيقات الفيدرالي أصرّ على استخدام 80 بت، بحيث يمكن بث مفتاح

الجلسة بالكامل. (ولربما كان ثمة بديل، يتمثَّل بالكف عن استخدام بعض بتات المفتاح، والسماح لمكتب التحقيقات الفيدرالي، بإتمام فك التشفير بواسطة هجوم بالقوة الغاشمة. وإذا ما تم، مثلاً، تحويل ثمانية بتات من مدى المفتاح إلىٰ ضبط المجموع، أمكن لمكتب التحقيقات الفيدرالي أن يتفحص مجرد 256 بديلاً مختلفاً ليجد المفتاح، لكن محاولة بليز لحل ضبط المجموع سوف تستغرق أكثر اثنتين وأربعين دقيقة، بل ما يزيد على أسبوع. وفي ذلك ضياع وقت طويل).

وفي غضون بضعة أيام، أرسل بليز مسودة أولية بنتائج بحثه إلىٰ زملائه في مختبرات بل. لكن معظمهم لم يستطع تصديقها، وسألوه: هل أنت متأكد من هذا؟» واقترحوا ضرورة مراجعة عمله من جديد. ولقد قام بذلك. ثم بدأ عملية مراجعة أكثر تدقيقاً وتمحيصاً بالاستعانة بأشخاص من الخارج. وذات صباح شمر بليز عن ساعديه وأرسل مسودة ما قام به بالفاكس إلىٰ فورت ميد. وبعد الغداء مباشرة أتاه الرد الذي يؤكد صحة استنتاجاته من الناحية التقنية.

سأله الشخص، الذي اتصل به من وكالة الأَمن القومي: «ما الذي تخطط له فيما يتصل بهذا العمل؟

أخذ بليز نفساً عميقاً. «أود أن أنشره».

ولقد أدهشه أنه لم يجد معارضة لذلك. بل إن القارئ في وكالة الأَمن القومي، أشار إلىٰ خطئين وقعا عند نسخ الأَرقام وخطأ نحوي واحد. والآن كان كل ما على بليز القيام به هو الحصول على موافقة الشركة التي تستخدمه، التي كانت تراهن بملايين الدولارات على الهواتف ذات المقراض. وبرغم وجود البعض الذين كانوا يرغبون في دفن البحث، استطاع بليز في النهاية إقناع رؤسائه، أنه من المستحيل إبقاء نتائج بحثه طي الكتمان، وبالتالي يجب ألاّ يفكروا حتّى بمجرد محاولة التكتم عليها. على أية حال، كانت أخبار هذا العمل قد تناهت إلىٰ سمع جون ماركوف، من صحيفة نيويورك تايمز. حصل

بليز على الموافقة بإرسال مسودة له، ليضمن دقة الرواية، مهما تكن القصة التي بلغته. واتصل ماركوف به ليحصل على بعض الإيضاحات. وبعد بضع ساعات عاد يتصل من جديد ووجّه سؤالاً غريباً لبليز: هل يعتبر قصته تستحق الاهتمام؟ لقد كان بليز يشعر بأنَّها كانت قصة جديرة بالاهتمام فعلاً إذ أظهرت كيف كانت وكالة الأَمن القومي مستعجلة لإخراج نظامها، وأكَّدت على مدى خطورة إكراه الناس على قبول شيء لم يبلغ النضج بعد. لكنها ليست قصة لتتصدر الصفحة الأولى أَو شيء من هذا القبيل. وبعد وقت قصير، اتصل ماركوف مجدداً، وهو يعتذر تقريباً، وقال أن اليوم فقير بالأخبار ولذلك فإنَّه سوف يخصص للقصة مكاناً أكثر بروزاً. وبناء على ذلك حسب بليز، أن الموضوع سيتصدر صفحة الأعمال التجارية.

كان قد سمع أن بوسع المرء الحصول على صحيفة اليوم التالي في التاسعة مساء من مبنى التايمز، ولشدة فضوله ذهب إِلىٰ هناك في ذلك الموعد. بعد أن تصفح الصحيفة بدقة وعناية، أصيب بخيبة أمل إذ لم يجد شيئاً. «لم يخطر ببالي حتَّى أن أنظر إِلىٰ الصفحة الأولى إِلىٰ أن خرجت من المبنى». لكنها كانت هناك تتصدر الصفحة كلها في المكان الأبرز من الصفحة الأولى، بعنوان «اكتشاف خطأ، في الخطة الفيدرالية للتنصت على المكالمات الهاتفية».

وكان لهذا مغزاه من عدة وجوه. أولاً، مع أن الخطأ ذاته يمكن إصلاحه ـ ويمكن المجادلة بأنَّه لم يعرض الأمن للخطر إِلىٰ حد بعيد ـ فإن الحقيقة القائلة بوجود ضعف كهذا ألحقت وصمة دائمة بنظام يعتمد على ثقة الجمهور. ولربما كان الأهم من ذلك أن حالة الركود السَّابقة، والكلام غير المفهوم عن الشّيفرة قد أبرزا هذه الناحية بحيث أن تطوراً معتدلاً مثل تفكيك بليز للشيفرة يمكن لمحرري التايمز النظر إليه على أنَّه القصة الأكثر أهمية في العالم ذلك اليوم. وما جعل هذا الموضوع الجاف مثيراً، كان ما فاح من رائحة الأخ

الكبير، الذي لم يستطع حتَّى، وضع برنامج بشكل صحيح. وقد أوقعت الحكومة نفسها في هذا الدور عن غير قصد، حينما أصر مسؤول متعجرف في وكالة الأَمن القومي، بأن هجوم بليز، بالرغم من أنه معقول، فإن تطبيقه عملياً بعيد الاحتمال، وهذا ليس ضمانة واضحة بشكل خاص، للقائمين على الشيفرة في البلاد. وكان أقوى من ذلك تأكيد مارتي هيلمان: «إن الحكومة تخوض معركة عسيرة».

وفي غضون ذلك، وبعد عدة مشكلات تتعلَّق بالتجهيزات الأولية، شرعت الحكومة في استخدام الهواتف ذات المقراض. (كانت رقائق القمة الأكثر شمولاً، والمصمّمة لضمان الاتِّصالات عبر الكومبيوتر، قد دخلت خط المعالجة منذ عهد قريب). وجرت العادة على أن يقوم أربعة رسل مزودين بتصاريح أمنية، اثنان من المؤسَّسة القومية للمعايير والتكنولوجيا واثنان من وزارة المالية، بالانتقال بالطائرة من واشنطن العاصمة إِلىٰ تورانس في كاليفورنيا، مرة كل أسبوع، إِلىٰ ما يسمى بمنشأة البرمجة بمقر إِدارة مايكوترونكس. (كانت الوفرة مقصودة شخصية لسلامة وتتفق مع بروتوكولات المستخدم في رقابة الأسلحة النووية). حين يصبحا في الداخل فإنهما ينتظرن محطة التشغيل صن حتَّى تنجز عملها، حيث تولد أولاً مفاتيح التشفير الفريدة التي سيتم إدخالها في رقاقات إم واي كي 78 MYK-78 (المقراض) ثم تقوم بتقسيم المفاتيح إِلىٰ جزئين وابتكار مجموعتين من الأقراص المرنة، في كل منها مجموعة من المفاتيح الجزئية. وإن تكوين المفاتيح الكاملة داخل الرقاقات يتطلب كلتا المجموعتين من الأقراص.

وإن إنتاج مجموعة الإسناد يتم بالطريقة نفسها. ثم يتم فصل الأقراص، وتذهب كل مجموعة منها ممهورة بخاتم بلاستيكي، مع اثنين من الرسل. وعندما يعود الرسل كل اثنين إِلىٰ الهيئة التي أرسلتهما، توضع الأقراص في خزائن مزدوجة الجدران وفق مقاييس الحكومة للمواد المحظورة. ويتم إدخال

مجموعات الإسناد إلىٰ خزانة أخرى. حيث تنتظر هناك، نحو 20,000 مفتاح مجزأ بحلول شهر أيار/ مايو عن عام 1994، وهي آمنة مطمئنة فيما حرب المقراض مستمرة.

في أواخر كانون الثاني/ يناير من عام 1994 وجّه العاملون في الكومبيوتر من أجل المسؤولية الاجتماعية رسالة إلىٰ الرئيس يحثونه فيها على إلغاء الاقتراح الداعي للأخذ بالمقراض، وشاركهم في التوقيع عليها خبراء في السرِّيَّة، ورجالات الصناعة، وأكاديميون، وكريبتوجرافيون، وأضيفت إليهم تواقيع أخرى تم جمعها عبر الإنترنيت. وفي غضون بضعة أشهر، فاخرت العريضة - إحدى أوائل الاحتجاجات السياسية عبر الإنترنيت - بأنَّها جمعت ما يزيد على 47000 توقيعاً. وفيما قد يرفض مرتاب هذا بالقول بأنّه جاء نتيجة حماس مبالغ فيه من الشبكة، فإن استطلاعاً للرأي أجرته النيويورك تايمز والسي إن إن أظهر أن الحكومة قد عانت هزيمة منكرة بحجم الهزيمة التي لحقت بالجنرال كستر [قائد عسكري أمريكي حارب الهنود الحمر وقتل بسبب سوء تقديره. هـ. م] في ميدان العلاقات العامَّة. إذ أن ثمانين بالمئة من الجمهور الأمريكي حالياً، يعارض المقراض.

لكن ذلك لم يكن له أثر يُذكر. فقد كانت الإدارة تراهن، على أن تحول أَنظمة التصدير، دون إدخال الشّيفرة المنيعة، في المنتجات التي يستخدمها الناس عادة، وستكون وديعة المفتاح هي الخيار الوحيد المتاح في الولايات المتّحدة. لكن الكونجرس كان يملك السلطة لتغيير تلك الأَنظمة. وأكثر من ساهم في الضغط في هذه المسألة، كانت امرأة عازبة في الثامنة والثلاثين من عمرها، تدخل الكونجرس للمرة الأولى.

كانت ماريا كانتويل ابنة سياسي من إنديانا. انتقلت إلىٰ ولاية واشنطن في العشرينات من عمرها، حيث عملت في المجلس التشريعي هناك، وفي عام 1992 فازت رغم الصعاب بمقعد في الكونجرس لتمثّل المنطقة التي تتألّف من

جزء من سياتل، والمدن الواقعة شرقي بحيرة واشنطن، وهي منطقة زاخرة بشركات التكنولوجيا المتقدمة، من نيتندو إلىٰ مايكروسوفت. ولذلك انصبّ اهتمامها، عند اختيارها لعضوية إحدى اللجان، على أحد المشاغل الرئيسة لصناعة البرمجيات، وهو التصدير، فتقدمت بطلب للانضمام إلىٰ لجنة الشؤون الخارجية ـ وعلى وجه التحديد لجنتها الفرعية، للسياسة الاقتصادية والتجارة والبيئة.

وكانت بالكاد قد ألفت الكونجرس لتجد حجرة إيداع المعاطف عندما وصلت أنباء الإعلان عن المقراض. وكان هذا مدعاة لإثارة غيظ ناخبيها من أصحاب كبريات شركات التكنولوجيا المتقدمة، وأخذت تمعن النظر في المشكلة وتتعمّق في دراستها، وخاصة ما يتصل منها بأَنظمة التصدير. وراحت تعمل عندئذ بشكل وثيق مع شركات البرمجيات التي تأثّرت بالإعلان، لا تلك التي في منطقتها وحسب مثل مايكروسوفت بل شركات أخرى أيضاً مثل لوتس. وكلما ازدادت اطلاعاً على أَنظمة تصدير الشّيفرة، كلما بدت لها شدة سخافتها في عصر الكومبيوتر. وقالت لسام جيجدينسون، رئيس اللجنة الفرعية وأحد ناصحيها التشريعيين: «لا يمكن أن يكونوا قصيري النظر إلىٰ هذا الحد ليحسبوا أن الكريبتوجرافيا سلاح حربي. وإذا ما استمروا على هذا المنوال فإنَّك لن تكون قادراً على الحصول على حماية على الإنترنيت».

وفي غضون ذلك، كان وضع التصدير قد بلغ حالة العطالة تماماً. وقام بعض قادة الصناعة الجديدة، مثل راي أوزي من لوتس وناثان مرفولد من مايكروسوفت ببذل جهود جبارة، في عام1992، وهم يتفاوضون مع وكالة الأَمن القَومي. وكانت تلك المفاوضات عبارة عن صدامات بين ثقافات متعارضة. وقد اعتبر رجال البرمجيات سعي الحكومة لإبقاء أجزاء من الشّيفرة داخل الولايات المتّحدَة نفسها موضوعاً مثيراً للسخرية، في حين أن خوارزميات الشيفرات تنتشر دون أي قيد في دول من ألمانيا إلىٰ روسيا. إن

الخطيئة الأكثر سوءاً هي التصرف غير المنطقي. أم أنَّه كان منطقياً؟ وفي إحدى المناسبات وجَّه مرفولد سؤالاً إلىٰ أحد الأشباح، في جلسة من جلسات المذاكرة: «ألا تدرك أنَّك في هذا أشبه ما تكون بصبي هولندي صغير، تحاول استخدام أصابعك لتسد خرقاً في سد أمام بحر من الشّيفرة المنيعة؟».

ابتسم الرجل المشاكس، وقال بتؤدة: «إن كل يوم يستمر فيه السدّ دون أن ينهار هو نصر». وكان ذلك صحيحاً. لا ريب في أن عفريت الشّيفرة قد أفلت من الزجاجة. لكنك إذا ما ألقيت في طريقه، مقداراً كافياً من العقبات، فإنَّه سيحتاج إلىٰ وقت طويل حتَّى يتمكن من الإتيان بعمل سحري.

أخيراً، أدَّت تلك الجهود التي بُذلت إلىٰ تسوية مؤقتة. فقد حصلت الشركات بالتعاون مع جماعة صناعيِة تُعرف باسم اتحاد ناشري البرمجيات، على الموافقة «لاعتبارات ملحّة» لتصدير برمجيات على أن يتم تقليصها وتغليفها لتباع لزبائن التجزئة. وكان الشرط الأساسي أن التشفير في تلك المُنتَجات سوف يكون بشيفرات رون رايفست آر سي ـ 2 أو آر سي ـ 4، واستخدام مفاتيح لا يزيد مداها على 40 بت. على أن يزداد هذا، كما يزعمون، في السنوات اللاحقة لمجاراة الكومبيوتر الأسرع. وفي المقابل، حصلت وكالة الأَمن القومي على قيود خاصة بها. لن يكتسب هذا النظام صفة رسمية بأن يعتمد معياراً بصورة صريحة. واضطرت شركة آر إس إيه والشركات الأخرى التي تستخدم الشيفرة لأن توافق على إبقاء تفاصيل تصميمها سراً.

ولم يلق هذا الاتفاق من يميل إليه بشكل خاص. إلاَّ أن المطروح أمام الشركات أحد خيارين: الأول أن تقدم، مثلما فعلت لوتس، للزبائن الأمريكيين نسخة بتشفير (64 ـ بت) المنيع، ونسخة أضعف للتصدير. عندئذ سوف يتساءل الزبائن الأجانب لماذا كانت برمجياتهم تقتصر على شيفرة من الدرجة الثانية، وفي بعض الأحيان، يشترون مُنتَجات أخرى. وقد ذهب راي أوزي إلىٰ الزعم، بأن هذا ما كان يحدث مع لوتس في ذلك الوقت. (وأطلق على الـ 40 بت كحد

أقصى اسم التشفير القابل للتجسس). أَو الخيار الثاني مثلما فعلت مايكروسوفت ويتضمن تجنّب متاعب التصنيع وشحن نسختين، بأن تقدم للجميع تشفيراً ضعيفاً. وفي غضون ذلك، شعر المتشدّدون في الحكومة، أن إعطاء الضوء الأخضر للسماح بالتصدير، مهما يكن طول المفتاح، فإنَّهم يكونون على منحدر زلق باتجاه شيفرة منيعة. قدموا لشركات مثل لوتس ومايكروسوفت أربعين بت الآن، فسوف تجدونهم يطرقون أبوابكم مطالبين بأَجهزة من ثمان وأربعين بتاً، وأكثر.

لكن عندما ذهب كانتويل وجيجدينسون إِلىٰ البيت الأَبيض، للمطالبة بالسماح بتصدير شيفرة أكثر قوة، ارتطما بجدار من الآجر. فقد وجدوا جماعة كلينتون ثابتين على موقفهم.

وفي تشرين الأول/ أكتوبر من عام 1993 عقد جيجديسون وكانتويل جلسة استماع للجنة الفرعية، ليلفتا الانتباه إِلىٰ المشكلة. قال جيجديسون: «إن جلسة الاستماع هذه مخصصة لمحاولات وكالة الأمن القومي الحسنة النية للسيطرة على ما لا يمكن التحكم به». كان يتحدث عن قوانين التصدير، لكنَّه ربما كان يتحدَّث عن أمر آخر ـ الدعم من الكونغرس الذي اعتبرته فورت ميد ذات مرة أمراً بديهياً. وبينما قبلت الأغلبية من أعضاء الهيئة التشريعية مزاعم وكالة الأَمن القومي، كما قدمها أصحابها، وكان ثمة تنافر معرفي أخذ يبرز بين ما كانت تسوقه من حجج وما بدا أنه نظرة للواقع أكثر قوة وإفحاماً. وقد عبرت كانتويل عن ذلك بوضوح في بيان الاستهلاك: «إننا هنا لنتبادل الآراء، حول رؤى متعارضة للمستقبل». من جهة كان ثمة مجموعة من العقول أسيرة الأوضاع التي.كانت سائدة أيام الحرب الباردة إِلىٰ حد أنَّها تجاهلت ما هو محتم ولا يمكن تجنّبه. ومن جهة أخرى كان هناك الحالمون التقنيون الذين زودوا مستقبلنا بالقوة المحرّكة، والتواقون إِلىٰ تدعيم الهيمنة الأمريكية في السوق العالمية.

كان أول شاهد في جلسات الاستماع راي أوزي، الذي جاء مجهزاً بنسخة عرض برمجية. وكانت لديه شاشة متصلة عبر خط هاتف بكومبيوتره في ماساتشوسيتس، الذي كان يستخدمه لاقتحام الإنترنيت وتنزيل واحد من «مئات الآلاف» من نسخ تطبيقات معيار تشفير البيانات المتوفرة وراء البحار. وقد وقع اختياره على واحد في ألمانيا، وقام بتنزيله في آلته خلال ثوان، كما يقوم بذلك أي شخص في العالم. لكنه، لاحظ، أنه إذا ما عمد عندئذ إِلىٰ إعادة البرمجيات ذاتها إِلىٰ ألمانيا، فسيجرم لقيامه بتصدير الشّيفرة المنيعة، التي يعاقب عليها القانون الفيدرالي.

أما الشاهد التالي فكان ستيف والكر، وهو مسؤول سابق في وكالة الأَمن القومي ويترأس الآن ترستيد أنفورميشن سيستمز، وهو مكتب استشاري، يساعد الشركات التجارية على تطبيق الشّيفرة. وقد عرض نتائج دراسة قام بها اتحاد ناشري البرمجيات حددت 264 منتج تشفير، يتم إنتاجها وراء البحار، 123 منها تستخدم معيار تشفير البيانات. وبإمكان الأجانب والشركات الأجنبية شراء أي منها، ولكن ليس مُنتَجات مماثلة تبتكرها الشركات الأمريكية لأن وكالة الأَمن القومي لا تجيز تصديرها. وقال: «لا يمكن أن يكون الأمر أكثر وضوحاً. إن وجود مُنتَجات تشفيرية واسعة الانتشار ومتاحة في الأسواق حقيقة ماثلة لا تقبل الجدل... إن حكومة الولايات المتّحدة نجحت في الواقع في شل قدرة صناعة أمريكية حيوية، وحسب». ثم أورد أمثلة معينة على صفقات تجارية أضاعتها شركات أمريكية، مثل إحدى الشركات التي أضاعت نصف زبائنها الأوروبيين بسبب عدم استطاعتها تزويدهم بشيفرة منيعة ومأمونة.

وبين فيل زيمرمان في شهادته، أن محاولة تقييد الكريبتوجرافيا، أشبه بمسعى لـ «تنظيم أمواج البحر والطقس». وشدّد دون هاربرت، المدير التنفيذي لشركة ديجيتال إكويبمنت كوربوريشن على القول بأن من الضروري أن تعدل

قيود التصدير في الولايات المتّحدة المفروضة على التشفير بحيث تتفق مع الواقع».

وكان أحد أعضاء اللجنة شخص لم يسبق أن عرف عنه الاعتراض على الحكومة، وهو محافظ من كاليفورنيا، يدعى دانا روهر باتشر، وقد نبه بصورة رسمية إِلىٰ أن ذلك لو وقع قبل خمسة أعوام، لقام بمعاقبة الشهود، لاستغلالهم وضعاً يحتمل فيه فقدان الأَمن القومي. لكنه الآن يقول: «إن الحرب الباردة قد وضعت أوزارها. وحان الوقت لكي نتقدم».

بعد الجلسة العامة، تفحص خبراء الأمن، القاعة بشكل دقيق، بحثاً عن أَجهزة تنصت، قبل جلسات المتابعة المحتومة، التي تمس مصالح وكالة الأَمن القومي، وقال جيجدنسون: «إن جلسة الاطلاع هي المكان الذي تجيب فيه وكالة الأَمن القومي على جميع تلك الأسئلة سراً». وكانت مطالعات وكالة الأَمن القومي ذات صيت سيء في دوائر الكونغرس. حيث تشتمل على عرض مؤثر توضح فيه الوكالة الأسباب التي تجعل قدراتنا على التنصّت الدولي، أمراً حيوياً إِلىٰ حد بعيد، وتتضمن كما هو مألوف تمجيداً بانتصارات تتحقق بالتطفل الخفي (انتصارات لم تكن ليتم التفكير بها دون رصد اعتمادات ببلايين الدولارات)، وأوضاع دولية محفوفة بالمخاطر تتطلّب يقظة ودعماً متواصلين. وكان بوبي إنمان، قد تولى إيصال الوكالة إِلىٰ حد الكمال حين كان مديراً لها»، ومنذ أيامه أدخلت الوكالة أعضاء من الهيئة التشريعية في عضوية جمعية «سري للغاية» فحولوا تحالفهم الضمني من المواطنين إِلىٰ وكالات الاستخبارات. وخلاصة الأمر أن عضو الكونغرس المنضم حديثاً إِلىٰ الهيئة التشريعية سوف ينال جرعة صريحة ومروعة من المعرفة بحقائق العالم، يفترض به أو بها بعد ذلك دعم أي مطلب تتقدَّم به وكالة الأَمن القومي وإِلاَّ نال «الهون البرابرة» من حريتنا بصفقة تجارية. وقد عرف عن أعضاء مجلس النواب والشيوخ دخولهم القاعة المنظفة من أَجهزة التنصت، والخروج منها بوجوه متجهمة، ليفاجئوا

مستشاريهم المتقدين حماساً، بقولهم: «حسن ربما يجب علينا أن نعيد النظر في الأمر».

لكن هذا لم يكن شأن ماريا كانتويل. إذ كانت بين عدد متزايد من أعضاء الهيئة التشريعيَّة الذين وجدوا مطالعة الوكالة مؤثرة إنما غير مقنعة. فالمسألة بالنسبة لهؤلاء المرتابين لم تكن مبلغ أهمية الشّيفرة وحسب، أَو النجاح الذي تحقق لنا بفك الشّيفرة، بل ما إذا كانت المحافظة على قوانين التصدير مثمرة حقاً. ثم ماذا لو أفلت العفريت من القمقم، ولم يكن بوسع الشركات الأمريكية بالتالي القيام بتصدير مُنتَجاتها؟ فإن المحتالين سوف يحصلون على الشّيفرة من أماكن أخرى!

بدأت كانتويل، بإعداد تشريع لعلاج هذه المسألة. فيما كانت لجنة الشؤون الخارجية، عاكفة في عام 1994، على وضع خطة للفحص الدوري الدقيق لأَنظمة التصدير. وقد أعدت كانتويل مسودة التشريع إتش آر H.R. 3627، «تعديل قانون إِدارة التصدير لعام 1979»، وهو مشروع قانون يضيف قسماً جديداً إِلىٰ القوانين القديمة، التي لها آثار معينة على الصادرات من البرمجيات، بما في ذلك التشفير. وبموجب هذا التشريع، يتم نقل سلطة القرار، من وزارة الدفاع إِلىٰ وزارة التجارة، وتجعل البرمجيات التي تم تقليصها وتغليفها والبرمجيات العامة مستثناة من أَنظمة التصدير. وهذا سوف يضع حداً للعبة وكالة الأَمن القومي بضبط الشّيفرة الأمريكية باستخدام قوانين التصدير.

بطبيعة الحال، لم يكن بوسع الإِدارة، أن تسمح بتمرير هذا التشريع المقترح. وعندما كانت كانتويل تتأهب لتقديم مشروع القانون أعلمها مستشاروها بورود مكالمة هاتفية من نائب الرئيس. وكان قد سبق لها أن اشتبكت لمرة واحدة، مع آل جور أثناء مناقشة الموازنة، حينما أيدت كانتويل، رغم تحفظاتها الشديدة، الإِدارة (وسوف ينتهي بها الأمر أخيراً إِلىٰ خسارة حملة إعادة انتخابها جزئياً بسبب ذلك). فما الذي يريده هذه المرة؟

قال: «أود أن توقفي مشروع القانون هذا». وكرّر الكلام الذي يتردّد في جلسات الاطلاع، بشأن الأَمن القومي وما إِلىٰ ذلك. تشبثت كانتويل بموقفها. وقالت: «إنني آسفة، يا حضرة نائب الرئيس، إنني أحترم رأيك، لكنني لن أبدِّل رأيـي».

وبطريقة ما، كانت تلك المحادثة، نقطة تحول لماريا كانتويل. فعملت على تمرير مشروع القانون إِلىٰ اللجنة الفرعية ثم واصلت الضغط ليفوز بالموافقة، على الرغم من أن الزملاء في اللجنة كانوا في ذلك الحين يحاولون حملها على التخلّي عنه. ولم تكن قد غادرت القاعة بعد التصويت ـ بل لم تكن نهضت من كرسيها بعد ـ حين صعد إليها أحد النوّاب وقال لها بصراحة: «إذا لم توقفي هذا، فإن الأمور سوف تصبح مزعجة جداً». وقالت ماريا كانتويل في نفسها: «لن أتوقف».

في 24 تشرين الثاني/ نوفمبر 1993، قدمت كانتويل مشروع القانون في قاعة المجلس. وكانت تعليقاتها فظّة، إذ قالت: إن نظام ضبط صادرات الولايات المتّحدة مفلس. وكان قد صمّم ليكون أداة في الحرب الباردة، للمساعدة على محاربة أعداء لم يعودوا موجودين. ولا بدّ أنّه لدى الوكالات الفيدرالية التي لا عدّ لها ولا حصر والمسؤولة عن ضبط تدفق الصادرات من بلادنا، شخصية جديدة تدرك حقائق يومنا هذا».

استمر الضغط، بالرغم من التعاضد، بين معظم الأعضاء في محاولاتهم لإقناعها. وثمة مثال على ذلك، حين صعد أحد زملائها الديموقراطيين إِلىٰ مكانها في قاعة اجتماعات المجلس وبدأ يوبخها بقسوة لتجاهلها مسائل الأَمن القومي. فشعرت حينذاك بالرهبة لكنها كانت على قناعة أكثر من أي وقت مضى بأن عليها مواصلة التقدم. ومع جميع القوى المحتشدة لمساندة قوانين التصدير العجيبة هذه ورقاقة المقراض السخيفة، وجدت الأمر تجلياً لسلطة لا تحدّها حدود ضد المستهلك.

ومع ذلك، كانت تعلم أنّها في المقدمة فيما يتعلّق بهذه المسألة. وبرغم أنّها كانت تؤدي خدمة جليلة، لقليلي الصبر الذين تمثّلهم، فإن معظم ناخبيها في الدائرة الانتخابية الأولى بولاية واشنطن كانوا يفضلون أن يكون تركيزها على قضايا مثل الرعاية الصحية، إلاّ أنها كانت هنا، حبيسة اجتماعات مع مستشار الأَمن القومي توني ليك. وبلغ مسامعها ذات يوم أن بيل جيتس سوف يزور المدينة. لذلك طلبت من أشخاص من مايكروسوفت ممن كانوا يعملون معها ـ ناثان مرفولد وبيل نيوكوم مستشار الشركة ـ إقناع رائد التكنولوجيا الأشهر في العالم بأن يمارس ضغطاً على زملائها من أجل القضية. وناشدتهما بالقول: إنني هنا في وضع حرج سياسياً. ودون دعاية إعلامية، جعلت بيل جيتس يخاطب لجنة الاستخبارات. وبدأت أدوات الأَمن القومي تشرح للمليارديرمدى أهمية قوانين التصدير، لكن مثال الاقتصاد الجديد كان قليل الصبر عند سماع المحاضرات. فأعلمهم أن ما بلغه منهم إن هو إلاّ تبرير سخيف. ولم يشعر أعضاء اللجنة بالاستياء، كانت متعة من نوع ما، أن يلقوا معاملة مزرية من أغنى رجل في العالم. ولا ريب بأن المرء لا يملك إلاّ أن يأخذه على محمل الجد، حينما يتحدَّث بشأن ما هو مفيد للفعاليات الاقتصادية.

وكانت لكانتويل مواقف مع البيت الأَبيض أيضاً. فقد طلبت من القوم هناك ألا يحاربوا مشروع القانون الذي اقترحته، بل أن يدعوه يأخذ مجراه في الكونجرس. وكانت الاستجابة غير متوقعة، وجاءت قبل التصويت بيومين وكانت عبارة عن صفقة. وأراد جماعة جور معرفة موقفها: إذا ما بدلنا موقفنا، فهل تسحبين مشروع القانون؟ واقترحوا أنّهم بدلاً من فرض رقاقة المقراض على الناس، سوف يؤيدون مشروعاً مختلفاً يقوم على إيداع المفتاح طواعية. وربما يكون مبنياً على تطبيقات برمجية، أكثر مرونة من الموجودة حالياً؛ وكذلك عوضاً عن أن تكون تسهيلات الوديعة لدى الحكومة وحدها يمكن أن يكون بعضها في القطاع الخاص، الذي هو موضع ثقة أكبر، مثل المصارف أَو شركات التأمين.

كان ذلك تراجعاً كبيراً، لكنه لا يزال في جوهره يتعلّق بمشروع الوديعة، وليس الحل النهائي الذي ترغب به كانتويل وناخبوها. ومن الناحية الأخرى، كانت حظوظ تمرير مشروع القانون الذي اقترحته من غير اعتراض، تعادل حظوظ شحن مايكروسوفت نظام تشغيل دون أَجهزة تنصّت. (حتى في ذلك الحين سيواجه رفضاً شبه محتم). عادت كانتويل إِلىٰ الأشخاص الذين كانوا يخوضون المعركة زمناً طويلاً قبل أن تنتقل إِلىٰ واشنطن. وتشجع بروس هايمان من المجموعة الصناعيّة التي تدعى اتحاد صناعة البرمجيات، على القول أن الحكومة كانت بذلك تقدم إطاراً لتسوية. واحتفل ناثان مرفولد بلا تردد. وقال لاحقاً: «لقد وهنت أعصابهم». واتفق مستشارو كلينتون جميعاً، مع ذلك، على أنه قبل سحب المشروع، يتعين عليها الحصول على وعود مكتوبة بما تم الاتفاق عليه.

في عصر 20 تموز/ يوليو 1994، قبل التصويت، وصلت رسالة من آل جور. وبعد الادعاء الفارغ المعتاد («إنني أكتب [هذه الرسالة] لأعبِّر عن تقديري الصادق لما تبذلينه من جهود، لدفع النقاش على المستوى القومي إِلىٰ الأمام. . .») ثم دخل جور في صميم الموضوع.

إن الإِدارة تتفهم ما يساور [أرباب] الصناعة من قلق، فيما يتصل برقاقة المقراض. وإننا نرحب بالفرصة للعمل مع الصناعة لتصميم نظام متعدِّد الاستعمالات، وأقل تكلفة. وإن نظام وديعة مفتاح كهذا سوف يكون قابلاً للتطبيق في البرمجيات، والبرمجيات الثابتة، والعتاد، أَو أي مركب من هذا القبيل، ولا يعتمد على خوارزمية محظورة، وسوف يكون طوعياً، وسيكون قابلاً للتصدير. . . كذلك فإننا ندرك أن نظام تشفير وديعة مفتاح جديد، يجب أن يجيز استخدام وكلاء لوديعة المفتاح من القطاع الخاص كواحد من الخيارات.

ومن الواضح، أن البيت الأَبيض كان يعتبر تلك الحركة، مجرد وسيلة

لتهدئة عاصفة محتملة من الغضب. (وفي وقت لاحق من الصيف، قيل لمسؤول في وزارة الدفاع كان يطلب توضيحاً عن الآثار المترتبة على تحول السياسة، بأن الرسالة إنما بقصد «استرضاء كانتويل الجمهورية وتجنّب طرح الموضوع للنقاش العام»). لكن حينما وجدت محتويات رسالة جور طريقها إِلىٰ الصفحة الأولى من الواشنطن بوست في اليوم التالي (إحراج طفيف لكانتويل، التي لم تكن تود أن تظهر وكأنَّها تؤدي مشهداً لإثارة الإعجاب)، وقد اكتشف جماعة جور من جديد بأن «بوسنة» الاتِّصالات [رقاقة المقراض]، كانت شائكة كعهدهم بها دائماً. لقد قطع البيت الأَبيض وعوده، دون أن يتم الاتفاق عليها مع وكالة الأَمن القومي ومكتب التحقيقات الفيدرالي. (وكانت المرة الأولى التي سمع بها كلينت بروكس يوم نشرتها الواشنطن بوست). تلقت كانتويل اتصالاً هاتفياً من أحد رجال جور. وسألها هل لديك مانع إذا ما، ألغينا الرسالة؟

أجابت قائلة: «أتعلم كم ستبدو سخيفاً؟ وبعد، لقد كانت تلك رسالة جور وكلماته. ووعدت بألا تستغل الحادث في الإعلام، لكن الأخبار كانت قد خرجت إِلىٰ العلن، ولم تكن لديها السلطة لأن تدعه يلغي الاتفاقية. فظلت الصفقة قائمة. وهكذا أسقطت كانتويل مشروع القانون الذي اقترحته، على الرغم من أنَّه في السنوات القليلة التالية سيكون الأول في عدد من مبادرات شعبية متزايدة في الكونغرس لإصلاح قوانين التصدير. وفي الوقت ذاته، فإن رسالة جور، سواء عن قصد أم لا، كانت برنامج العمل الأساسي الذي ستعتمده الإِدارة في التعامل مع رقاقة المقراض سيئة الحظ. خطوة إِلىٰ الوراء. رفض، خطوة أخرى إِلىٰ الوراء. عرقلة واضطراب، بينما النقاش العظيم الصادق الذي تخيله كلينت بروكس بشأن سياسة تشفير قومية، لم يتقدم إِلىٰ الطليعة قط. وفي الوقت ذاته، فإن الخطة التي اعتبرها بروكس أساسية جداً، حلاً تشفيرياً كاملاً لحماية السرِّيَّة، سياسة ستولد سياسة التوقيع الرقمي الشامل، لتقوية التجارة الإِلكترونية ومنع التزوير الإِلكتروني، ومدخل لتطبيق القانون، لم تلق الدعم الصريح.

أراد كلينت بروكس أن يخرج من الصراع. فبعد سنتين من التردد بين ماريلاند والعاصمة، والدخول في المناقشات ذاتها مع الأشخاص أنفسهم، سأل المدير الجديد لوكالة الأَمن القومي إن كان بإمكانه، القيام بأي شيء يفيد من مواهبه بكفاءة أكبر. ولقد قبل طلبه وتلاشت النيرفانا.

جرّ الخطى نحو التشفير

كان واضحاً حين أطل عام 1995، أن ميدان الكريبتوجرافيا ـ بكل أبعاده ـ قد تبدلت ملامحه بشكل مؤثر، بالرغم من كل ما بذلته الحكومة من أفضل جهودها لإبقاء الأمور على استقرارها. فقد كانت تقنية التشفير، مندفعة بقوة الكومبيوتر والاكتشافات الجديدة التي طلع بها أمثال هويت ديفي في العالم، تتحرّك بسرعة المحرك التوربيني، منتقلة من عربة السفر التي تجرها الجياد إِلىٰ زمن الإنترنيت. فبالرغم من التذكير المتزايد باطراد بشبح انتشار فوضى التشفير، حيث تنتشر الرموز وتفلت من عقالها إِلىٰ حد لا تستطيع معه حكومة أَو مؤسَّسة أن تأمل في معالجة تجارة رقمية أَو قانون، فقد استمر الصراع القديم بين الإجراء ونقيضه. إن الغرباء وحدهم الذين لهم يد في هذه اللعبة.

قبل قرن ونيف كان إدجار ألان بو قد أصبح شبه مأخوذ بموضوع علم الشيفرة فكتب: «يمكن التأكيد مرة أخرى أن العبقرية الإنسانية، لا تستطيع أن تركِّب شيفرة، يستعصي على عبقرية الإنسان أن تأتي بحل لها». من الناحية الرياضية كان بو على خطأ؛ فورق الحل لمرة واحدة التي عُرفت بمناعتها في محاولات الاختراق هي اللازمة الشعرية التي تفيد بأن زعمه مضى وانقضى إِلىٰ غير رجعة. وفوق هذا وقبل كل شيء كان تنفيذ ورقة الحل الوحيدة أمراً مجهداً

لمن يتصدى له؛ وهو بالتأكيد غير مناسب في التطبيق إذا كان نطاق العمل واسعاً. وإذن هل كان الشاعر، من الناحية العملية، مصيباً في ما ذهب إليه؟ وكان مذهب مارتين جاردنر حين اقتطف قول بو في مقاله الشهير عن الخوارزمية رسا في مجلة العلوم الأمريكية Scientific American، أن الشاعر أخطأ في ما ذهب إليه.

إن السؤال قد أثار بلا ريب شجون فيل زيمرمان. فقد كان يشعر في أعماقه، أن خوارزمية التشفير في صميم برنامجه «منتهى السرِّيَّة» بي جي بي سليمة متينة. ولذلك حين فكّر بتسمية البرنامج اختار هذا الاسم، والحق أنه يمكن لمستخدمي هذا البرنامج أن يطمئنوا إلىٰ منعته أمام محاولات من يعملون في تفكيك الشيفرات. وقد أشارت الحكومة أيضاً إلىٰ متانته، في تصريحاتها العلنية على الأقل. ففي ربيع عام 1995 شهد لويس فريه من مكتب التحقيقات الفيدرالي ووليم كرويل من وكالة الأَمن القومي في جلسة استماع سرِّيَّة في الكونجرس بأن من الصعب تفكيك الرسائل المشفَّرة بمفاتيح طويلة. وكانت شكوى فريه أنه ليس لدى [مكتب التحقيقات] لا التكنولوجيا ولا القدرة على استخدام القوة الغاشمة لبلوغ هذه المعلومات». أما كرويل فمضى إلىٰ أبعد من هذا، إذ قال، مستنداً إلىٰ التطورات الراهنة التي بلغتها تكنولوجيا الكومبيوتر الشخصي، أن «تفكيك رسالة مشفرة بمفتاح من 128 بت، الذي يستخدمه برنامج «منتهى السرِّيَّة» بي جي بي يستغرق 8,6 تريليون أمثال عمر الكون».

ولكن زيمرمان كان يعلم أن هجوماً بالقوة الغاشمة، على خوارزمية آيديا International Data Encryption Algorithm IDEA ـ خوارزمية تشفير البيانات العالمية ـ ليست الطريقة الوحيدة لتحويل شيفرته إلىٰ ما يمكن وصفه «بمحاولة جيدة لبلوغ السرِّيَّة». فقد كان هناك ما لا يحصى من الطرق لتفكيك الشيفرة. ولربما كان بالإمكان إنجاز عمل المفتاح العام من البرنامج بخوارزميات أشد فاعلية في تحليل العوامل وعتاد كومبيوتر ضخم أقوى. أو قد يكون في تفاصيل

تنفيذ برنامج «منتهى السرِّيَّة» مثالب، وهذا أرجح، توفر لمحلل للشيفرة طريقاً مختصراً للوصول إِلىٰ النص الأصلي الواضح.

ولقد شاءت الصدفة، أن يجتمع بضعة من الاختصاصيين بالشّيفرة ذات مساء في مؤتمر لهم سنة 1995، في سانتا بربارة، وهم في زيهم التقليدي من قمصان رياضية، وينتعلون الصنادل، وأخذوا يتحلّقون حول أحد المتحدثين البارزين في تلك الليلة. وكان هذا روبرت موريس الأب، ولم يسبق له أن حاضر في جميع، إلاَّ اللهم من كان مخولاً بالاطلاع على أسرار الحكومة الأمريكية. وكان موريس قد تقاعد لتوه، وهو في منصب كبير العلماء في فورت جورج ميد. فاجتذبتهم شهرته، وقد باتت ضخمة بسبب الإنجازات التي تنسب إليه ولا سبيل إِلىٰ معرفتها لأنها في خدمة مملكة الأشباح إِلىٰ طاولته. ولما ذكر أنه لا يمانع في لقاء فيل زيمرمان، أسرع من ينادي الرجل ذا للحية المشذبة والحادي والأربعين من العمر.

بادره رجل المخابرات السابق ـ وهو ينفث دخان سيجارته بشدة ـ بالحديث: «دعني أطرح عليك، يا فيل، سؤالاً. لنفترض أن زيداً من الناس استخدم [برنامجك] «منتهى السرِّيَّة»، لبث رسالة يترتب عليها ضرر شديد. فكم ستكون كلفة تفكيكها؟».

أجاب زيمرمان، وقد بدا عليه الضيق: «قد سبق أن وجّه إليَّ هذا السؤال من قبل. وردي هو أن ذلك ممكن».

«ولكن كم ستكلف؟».

كان هذا الموضوع بعيد كل البعد عن الموضوعات الأثيرة لدى زيمرمان، إلاَّ أنه قبِل بمسايرة محدِّثه. فقال على سبيل التخمين أن الاعتماد على حجم المفتاح ليس السبيل الأفضل لشن الهجمات على برنامج «منتهى السرِّيَّة»، بل الأجدى العناية بنقاط الضعف الأخرى. وذهب إِلىٰ أن المرء قد يجد اضطراباً في بنية البيانات، كما أن في تقويم الأخطاء فيها ضعف.

هز موريس رأسه ولم يعلق بكلمة. فمن ذا الذي يعلم إن كانت وكالة الأَمن القومي قد اكتشفت فعلاً عيباً بسيطاً أتاح للمساحات الكبيرة من السيليكون في القبو العتيد في مقرها لفظ النص الواضح الأصلي الذي بثّه المناضلون الأحرار الذين يُزعم بأنّهم يستخدمون برنامج زيمرمان؟ ولكن في اليوم التالي ضمن موريس في حديثه تعليقاً مواربًا على علماء الشّيفرة الجدد ورؤاهم الفوضوية للشيفرة. ولم يكشف في ذلك أية أسرار مهنية، لكنه بروح حكماء الشرق قدم حكمتين تصدقان في كل زمان ومكان ـ قولان من عقيدة الشّيفرة ـ تومئان إِلىٰ المصالحة التي لا بد أن تتحقق بين «المنصفين»، وهي مصلحة تتجاوز الصراعات السياسيَّة الراهنة. وكانت تلك لمحة من مشهد مجتمع ما بعد المقراض في القرن القادم.

القول الأول (الموجه إِلىٰ مفككي الشّيفرة): لا تقلّل من تقدير عزم خصمك على بذل المال والوقت لتفكيك الشّيفرة التي تستخدمها. وكان جوهر حديث موريس أن من الأفضل أن تدع الكريبتوجرافيا لذوي العقل الذي يحكمه جنون البارانويا، أولئك الذين يؤمنون إيماناً قاطعاً جازماً بأن خصومهم مجرد قوم ذوي ثراء فاحش وذكاء شديد وعزيمة ماضية، كلاب صيد تجري في أثر الطريدة. وهؤلاء سوف يشنّون هجمات مباشرة على شيفرتك المعتمدة، وغالباً ما ينتصرون.

القول الثاني (الموجّه إِلىٰ مفككي الشّيفرة): ابحث عن نص أصلي واضح. وكان هذا طمأنة للحاضرين، بأنَّه مهما بلغ تفكيك النَّص من الصعوبة الشديدة، فإن الحقيقة هي أن الذين يناط بهم أمر هذه الأَنظمة المعقدة، إنما هم بشر عاديون. وهكذا، قد تتضمن شيفرة تبدو مستعصية على الاختراق، خليطاً من قصاصات من الشيفرة القياسية الأمريكية، لتبادل المعلومات ASCII على المرء أن يطوعها لتخرج بلغة البشر، فيقع فيها المرء من حيث لا يتوقع على

مقطع أَو رسالة كاملة غير مشفَّرة، إن سهواً وإن مصادفة. فيمكنك أن تطالعها بأيسر ما يكون.

كان موريس يقول لفوضويي الشّيفرة: «حذار، فليس سهلاً أن تقيموا عالم شيفرة مثالياً». وهكذا تدور اللعبة القديمة. ولكنه بإلقائه الدرس على الغرباء كان يقر ضمناً بأن المستقبل ليس حكراً على حكماء وكالة الأَمن القومي، وإنما هو من شأن هؤلاء ذوي الشعر المسترسل، الذين يرتدون القمصان الرياضية في سانتا بربارة أيضاً.

لقد صدرت أقوال موريس، في وقت كان التوتر فيه على أشده بين الشّيفرة الشعبية والشّيفرة الحكومية، وزاد في الطين بلةً ظهور تحول مستمد حديثاً، فبعض القوى الصاعدة في مجال التشفير كانت قد تجاوزت الترميز، وغاصت عميقاً في تحليل الشيفرة؛ وفي حين أن هذا أمر نهض به حشود المهتمين بالتشفير من قبل، والأشهر في هذا يتجلّى في الهجمات على خطة ميركل المسماة الحقيبة المتعددة التكرارات، ظهر الآن نوع من الجهد جديد كل الجدة، ولا يمتثل للقواعد التقليدية التي صيغت في عالم وليم فريدمان أَو ألان تيورينج. . . وكان هذا تفكيك للشيفرة يقوم على التراكم، أي جهد ضخم مشحون بالقدرات المضخمة التي تتسم بها الشبكة وكان رواد هذا المجهود هواة الشّيفرة، طبعاً. ولم تكن هذه السلالة من مفككي الشّيفرة لتعنى بالجريمة أَو التجسّس، وإنما لطرح فكرة سياسية، وتحقيق أقصى المتعة.

بدأت أولى هذه الجهود ببرنامج «منتهى السرِّيَّة» بي جي بي، الذي طلع به فيل زيمرمان. وكان مستخدمو هذا البرنامج، قد شغلتهم شكوكهم الملحة بمتانته طويلاً قبل أن يثير موريس التساؤل حوله في مؤتمر الكريبتو 95. وقد عكس هذا القلق الأساسي الذي يشغل بال الكريبتوجرافيا الثورية: هل تستطيع أن تثق ببرمجيات طورت بدون ترخيص من مؤسَّسة مشهود لها بإنتاج الشيفرات المأمونة؟ كان هذا هو السؤال، الذي طرحه على نفسه ديريك أتكينس، وهو ما

يزال طالباً في العشرين من عمره، على مقاعد الدراسة في كلية الهندسة الكهربائية في معهد ماساتشوسيتس، سنة 1992. وقد كان رد فعله المبدئي على مشروع زيمرمان الانضمام إِلىٰ الحملة الدائرة، ثم غدا عضواً في فريق التطوير الذي تكون بصورة عفوية لابتكار أشكال جديدة من البرمجيات. وأخذ اتكينس بعدئذ يتساءل أي شكل من الهجمات يمكن أن تؤثر في تلك البرمجيات.

وكما أشار بوب موريس في حديثه، فقد كان ثمة طريقتان لتفكيك نظام للتشفير: الأولى بالقوة الغاشمة، أي أن تتوسل بكل الحلول الممكنة، حتى تعثر على الحل الصحيح. والثانية تتطلب البحث عن طريق مختصر، أي نقطة ضعف غير مقصودة قد تتيح لك تفكيك رموز الرسالة المشفرة. وكان أن اختار اتكينس، بعد أن خاض في الموضوع مع أصدقائه ـ ومنهم مايكل جراف الأستاذ في جامعة آيوا ستيت. وبول ليلاند بجامعة أكسفورد ـ أن يسلك الطريق الأول في الهجوم. ولكن محاولة العثور على ثغرة أَو عيب كانت أمراً يتجاوز طاقاته أَو تجربته. (مع أن هذا الطريق الذي حاولت الوكالة، كما ألمح موريس، أن تعرفه على الأرجح). ومن جهة أخرى، بدا الجميع متفقين على أن الخط المباشر، وربما الممكن، لتفكيك برنامج «منتهى السرِّيَّة PGP» هو الطريق الذي يسير عكس أي برنامج يستند إِلىٰ خوارزمية رسا: أي طريق تحليل العوامل.

كان رايفست وشامير وأدليمان قد أدركوا، أنه إذا اكتشف المرء طريقة سريعة لتحليل العوامل: رأي تعيين العددين الأوليين الأصليين اللذين جاء المفتاح من حاصل ضربهما، فإن نظامهم يصبح غير ذي جدوى. ولئن كانوا يتوقعون ظهور خوارزميات أفضل لتحليل العوامل فقد كان الفكر يزين لهم أنَّه ليس هناك في الأفق، ما يعد باحتمال تفكيك خوارزمية رسا. ومع ذلك فقد شاء اتكينس وأصدقاؤه امتحان هذه الفكرة. وجنحوا يومذاك إِلىٰ الظن بأنَّهم باعتمادهم على مصدر لم يكن متوفراً من قبل ـ أي آلاف الكومبيوترات المتوفرة

للناس الذين يتصلون بالإنترنيت ـ قد يستطيعون أن يبدأوا تاريخاً لتحليل العوامل. وكانت تلك حجة آسرة، من حيث قوة الحساب المتضاعفة لمستخدمي الإنترنيت بما يجعلها أشبه بسوبر كومبيوتر عملاق، ولعل هذا هو ابن عم لتلك الكومبيوتر المفترض أنّها موجودة في قبو فورت ميد. ولقد طرحوا الفكرة على أرجن لينسترا، عالم الرياضيات الخبير بجامعة بيلكور في نيو جيرسي. فكان جوابه أن الأعداد الأولية الضخمة المستخدمة عموماً في «منتهى السرِّيَّة» (والنسخ التجارية من خوارزمية «رسا»)، أضخم من أن ينجح معها هجوم. ثم اقترح عليهم تحدياً آخر: الخوارزمية رسا 129.

ولقد بلغت فكرة لينسترا قلب القضية مباشرة، وهي هل يمكن للكريبتوجرافيا (التشفير) أن تكفل الأمان الكامل. وكان التحدي الذي يتجلى في «رسا 129» هو الذي طرحه مارتين جاردنر في عموده في مجلة العلوم الأمريكية عام 1977 ـ فالعمود الذي بدأ باستنكار قول [الشاعر إدجار الان] بو، أنه ليس هناك من شيفرة حصينة منيعة لا تلين إذا ما هوجمت. وظل هذا التحدي قائماً لا يجد من ينهض له طوال تلك السنين، وقد قدر الزمن الذي يستغرقه كومبيوتر جبار متفرغ لتحليل العوامل لرقم بهذا الحجم 40 كودريليون سنة. ولكن حتى وإن لم تقبل بهذا الرقم (ورايفست يقول الآن أنه كان خطأ رياضياً) فإن عدداً دون ذاك بكثير ـ ولنقل بليون أو بضعة ملايين من السنين ـ يعني أن من يتنفس اليوم، سيكون قد صار هباء منثوراً منذ عهد بعيد قبل أن يظهر سر رسالة مشفرة بخوارزمية رسا مؤلفة من مفتاح من 129 رقماً.

ومع ذلك فقد جمع اتكينس وجراف وليلاند ولينسترا بعد خمسة عشر عاماً قواهم مع الإنترنيت، للفوز بالمئة دولار في غضون شهر.

كان أول ما احتاجه هؤلاء، وربما الأهم، هو خوارزمية جيدة لتحليل العوامل. وكانت قد تحقَّقت بعض التطورات النظرية في هذا المجال منذ أن نُشر مقال جاردنر، ويخص بالتنويه ما ابتكره أحدهم، وهو «انحراف غربال

الممدد التربيعي لعدد أولي كبير مضاعف متعدد الحدود». وهذا يتضمن بحثاً في عالم الأعداد يعرف بالفضاء المتجهي Vector Space لأعداد تُعرف بـ«الشعاع الأحادي» Univector. ويمكن رسم العلاقات الرياضية، بجمع هذه الأعداد، على نحو يؤدي إلىٰ معرفة الكثيرين الأوليين الأصليين. «وليس عليك، كما يقول اتكينس، أن تستقصي كل مجال الاحتمالات، بل حسبك جزء بالغ الصغر من الفضاء. ولك أن تشبه الأمر بأننا كنا نبحث عن ثمانية ملايين إبرة في تل من القش مليء بما لا يحصى من الإبر، وإن لم تكن تبحث عن إبرة بعينها، وإذن حسبك من الأمر أن تجد ما يكفي من هذه الإبر ثم تقوم بجمعها بوسيلة رياضية معينة، بما يساعدك على تحليل العدد إلىٰ العوامل الأولية التي يتألف منها». وقد كان هذا الأسلوب مثالياً لهجوم إنترنيتي موزع حيث تتجمع قوى مئات الناس مع بعضها البعض لحل المعضلة».

في صيف 1993، كان البرنامج قد تم واكتمل، وكان اتكينس يجري هذا البرنامج على كومبيوترات مخابر الإعلام في معهد ماساتشوسيتس، وبات بالإمكان بعد هذا، تجنيد المتطوعين مع الكومبيوتر. وكانت الاستجابة عظيمة، إذ أخذ أكثر من 1600 آلة بالعمل في حل المسألة، على امتداد العالم، وفي كل قارة عدا القطب المتجمد الجنوبي. وقد تفاوتت هذه الكومبيوترات من حيث الحجم، من الكومبيوتر الشخصي الصغير، حتى السوبر كومبيوتر ماسبر المعالج 16000 في مخابر بل.

تقاس قدرة الكومبيوتر بمليون أمر MIPS في العام ـ أي أنه آلة تستقبل مليون من التعليمات في الثانية على مدار العام. وقد استخدمت في تجربة خوارزمية «رسا 129»، ما بين أيلول/ سبتمبر 1993 ونيسان/ أبريل 1994 حوالي خمسة آلاف من أعوام MIPS هذه. وكان في تلك الفترة أن فطن اتكينس والآخرون إلىٰ أنّه بات لديهم ما يكفي من الأشعة الأحادية للقيام بالحسابات

النهائية. فبعثوا بها كما كان مخططاً إِلىٰ لينسترا في مخابر بل Bell Lab، الذي تولى «اختزال المصفوفة» النهائي. كذلك أرسل اتكينس للينسترا شريطاً يساوي 400 ميجا بايت من الأشعة الأحادية بالبريد العادي. وأرسل بعد شريطاً إضافياً عن طريق فيدإكس Fedex. فقام لينسترا بتلقيم آلته بهذه البيانات، وتم اختزال المصفوفة في غضون يومين. وفي يوم 24 نيسان/ أبريل 1994 بعث الرسالة التالية عبر الشبكة:

يسرنا أن نعلمكم بأن

ولقد استطاع نقل هذه الرسالة، بإدخال المفتاح في العدد الذي يمثل الرسالة المشفرة، لتصبح هذه بدورها عدداً طويلاً كسابقتها. ثم كان أن نقلت هذه الرسالة إِلىٰ الإنكليزية بسهولة بواسطة أقدم طرق فك الشيفرة في التاريخ: 1. = أ، 2. = ب. وهكذا. وبذلك تم كشف السر الذي يفترض أن يستغرق جلاؤه كوادريليون سنة.

الكلمات السحرية هي صقر السمك المتقزز.

وقد يتساءل المرء هل اهتز عالم رون رايفست بهذا الاكتشاف؟ الحق أن عالمه ذاك لم يتأثّر كما قد يخال المرء. فقد ظل يتابع في السنوات التي أعقبت نشر مقال جاردنر التطورات في تحليل العوامل، وخلص إِلىٰ أنه ليس من المستحيل أن يأتي اليوم الذي يخرج من الدفتر شيكاً بمبلغ مئة دولار التي رصدها جائزة. (والغريب في الأمر أنه نسي نص الرسالة). بل إنه يدافع عن نبوءة جاردنر التي استبعد فيها تفكيك الرسالة في حياتنا: «ربما كان دقيقاً حينذاك بالنسبة لتحليل أسرع خوارزمية نعرفها، غير أن التكنولوجيا كانت تتحرّك بسرعةٍ على حدود تحليل العوامل».

لكن القول «حدود تحليل العوامل» كان كافياً في حدّ ذاته، لإثارة قدر من الشك لأمان أشد مفتاح عام للشيفرة شيوعاً وشعبية. فإذا كان تحليل العوامل يسيراً فسوف تكون الخوارزمية رسا في المحصلة غير ذات قيمة. ولقد كان

تفكيك الخوارزمية «رسا 129» أبعد ما يكون عن الصعوبة، مقارنة برموز الرسا المستخدمة في النشاط التجاري. فعندما يستخدم نظام الرسا 129، عدداً يكون طول المفتاح 245 بت. لكن مفتاح الرسا المعياري ـ وهو الذي تستخدمه برمجيات الشركة ـ كان طوله 1024 بت. ولو كان فريق اتكينس يقوم بالعمل ذاته بمفتاح بذاك الطول لكانت كومبيوتراتهم ما تزال تعمل على حلّ المعضلة، لأمد من بضعة ملايين أخرى من السنين.

ومع ذلك فقد كان هذا العقم متوقعاً للرسا 129. فهل يمكن للتقنيات الجديدة في تحليل عوامل الأرقام أن تذوب أثخن مفاتيح الرسا؟ قد يكون هناك فتوحات في الرياضيات يمكن بها تسريع تحليل العوامل، إلاَّ أن الخطر الأعظم على قوة أنظمة التشفير برز مع تطوير ما يُعرف بالكومبيوتر الكمية Quantum Computers، وهي آلات تفيد من فيزياء الجزئيات، لتجري بسرعة أعظم مما تعمل به النماذج الحالية. (قارن فارق السرعة بين السلاحق وأشعة الليزر). وكان العلماء يخطون الخطوات الصعبة لتنفيذ هذه الكومبيوتر بعد أن كانت موضوعاً نظرياً. فإذا تمت الرحلة وخرجت الكومبيوتر الكمية صار بوسعك عندئذ أن تضرب صفحاً عن نظام «الرسا» في التشفير. وهاك ما كتبه الكريبتوجرافي جايلز براسارد في عام 1996: «أعتقد أنني سوف أرى في حياتي أداة كمية خاصة لتحليل العوامل. فإذا تحقق هذا فسوف يكون هجر «الرسا» واقعاً. «وقد ورد هذا، في نشرة كريبتو بايتس التي تصدرها آر إس إيه داتا سيكيوريتي.

ولكن ذلك ظل من قبيل الحدس. أما الواقع فهو أن ديريك اتكينس وزملاءه التقطوا ما بدا لهم مسألة مستعصية على الحل واستطاعوا تفكيكها، دون أن يجمعهم جامع رسمي، وبواسطة مجموعة متنوعة من الكومبيوتر، كيفما اتفق. وخلاصة ما قاله: «ما تعلمنا هو أنّه بوسع مجموعة من الهواة أن يجتمعوا معاً وينفذوا هذا الأمر». أما المزاعم ونسبة العصمة فينبغي النظر إليها بعين الشك.

أما الهدف التالي فكان لا يقاوم: نظام تشفير من 40 بت سمحت الحكومة بتصديره. والموضوع هو محض سياسي هذه المرة. إذا تم توجيه أسلوب حشد القوى الذي استخدم في تحليل الرسا، ضد ذلك المفتاح الضعيف الذي كان مدار التفاوض مع اتحاد ناشري البرمجيات عام 1992 (ولم يعدل في السنوات اللاحقة، بالرغم من الوعود التي قطعتها الحكومة)، فإن ذلك المفتاح مصيره السقوط، ولسوف يكون من الواضح الجلي الحاجة إلىٰ نظام تشفير أقوى.

وبعد أن طرح أحد زعران الشّيفرة فكرة «حلقة لتفكيك المفتاح» حثّ تيم ماي على القيام بعمل، معتقداً أن قدرة «وحدة المعالجة المركزية CPU في هذه القائمة» قابلة للاستغلال على نحو مؤثر في تفكيك المفتاح خلال ستة أشهر (المدة ستة أشهر نتيجة التخمين. ولكن مقارنة الجهد الحسابي اللازم لها بتفكيك خوارزمية الرسا هي أشبه بالمقارنة بين المفتاح والبرتقال ـ استقصاء مدى المفتاح مقابل تحليل العوامل).

كتب آدم باك، وهو شاب في الخامسة والعشرين يدرس علوم الكومبيوتر بجامعة اكستير في إنجلترا: «تمهلوا، فلقد كنت قطعت فترة في هذا العمل. . .». وكان قد بدأ بكتابة النصوص، بُعيد اطلاعه على أول إرسالية، ليتيح للناس المشاركة في تفكيك الشّيفرة جماعياً. كان يدرك ما هو بصدده، لأنه كان يعالج قبل حين الخوارزمية آر سي ـ 4 ـ الشّيفرة الحقيقية التي نفذت التشفير في 40 بت المسموح بتصديرها من الحكومة ضمن برامج مايكروسوفت واللوتس.

إن الهجوم بالقوة الغاشمة على شيفرة منفذة ككتلة مثل الآر سي ـ 4 أَو معيار تشفير البيانات يتطلب من المفكّك معالجة النص بكل تركيبة رقمية ممكنة. كذلك يتطلب العثور على المفتاح البحث في كل مجال الاحتمالات؛ وهناك في حالة المفتاح المركب من 40 بت، حوالي تريليون احتمال مما يكفي

لتشغيل دستة من الكومبيوتر أياماً بطولها، ليتم العثور على المفتاح. وهاك ما كان يدور في عقل آدم باك: جهد يقوم به عدة أشخاص، ولكل منهم جزء من حيز المفتاح يقوم باختباره، ثم يتوسع في البحث. وتستمر هذه العملية حتى يعثر أحدهم على المفتاح. فيقوم بإرسال نصوصه إلىٰ صفحة الشبكة فيتنادى مجموعة من المتآمرين من مختلف أنحاء العالم بسرعة للاجتماع. وفي النهاية يحاول تسعة وثمانون من زعران الشّيفرة العثور على مفتاح من 40 بت في برنامج مايكروسوفت Access أكسيس القائم على إدارة قاعدة البيانات.

ولكن محاولة التدخّل في برنامج مايكروسوفت أكسيس فشلت؛ إذ لم ينجح أي من ملايين المفاتيح المحتملة في فكّ الرسالة، بالرغم من «اجتياح» كامل حيز المفتاح. وتبين أن من حاول التلصص قد اصطدموا بنقطة فنية حالت دون حصولهم على النّص العادي، (يقول باك في هذا أن المشكلة كانت في الافتقار للمواصفات، فلم نكن نعلم الشكل الذي كان عليه الملف).

ومع ذلك فقد خرج زعران الشّيفرة، من الهجوم الفاشل على برنامج مايكروسوفت بشيء من برمجية اختراق جماعي، أي تنظيم فضفاض إنما مثابر في جهوده ورغبة مستمرة في الكشف عما كانوا يعتقدون أنه غش يدعو للأسف في التشفير المُعد للتصدير. ثم وقع زعران الشّيفرة عندئذ على هدف أفضل لشنّ هجوم بالقوة الغاشمة: نيتسكيب.

في عام 1993 جلس طالبان من جامعة إيلينيو، يتبادلان الحديث في أحد المقاهي، وكان حديثاً لم يغيِّر مجرى الشبكة العالمية، الإنترنيت، التي مضى عليها اثنان وعشرون سنة، وحسب وإنما كان له أعمق الأثر في الأخذ بالتشفير. كان أحدهما طالب جامعي قصير القامة بدين يدعى مارك اندريسين، وقد عرف حديثاً بنظام جديد على الإنترنيت أطلق عليه مخترعه عن رعونة اسم وورلد وايد ويب World Wide Web (شبكة العالم الفسيح)، وكان ذاك المخترع يدعى تيم بيرنرز ـ لي، وهو عالم كومبيوتر بريطاني يعمل في سويسرا. وكان نظام ويب

هذا طريقة فذة للطباعة والوصول إِلىٰ معلومات عبر شبكة الإنترنيت، غير أنه لم يكن يأخذ بهذا النِّظام سوى قلَّة من طائفة الفنيين الاختصاصيين. ولكن أندريسين وجد في هذا النِّظام إمكانية أوسع للإفادة منه. وعبَّر عن ذلك بما قاله لزميله إيريك بينا: إذا ابتكر أحدهم «متصفحاً» زلقاً ليجول في فضاء المعلومات الذي تكون بفعل حشد من الناس الذين يشاركون في نصوص وصور وأصوات على شبكة الويب فسوف يكون من الأيسر استخدام الإنترنيت ذاتها وتصبح طريقة أفضل للحصول على المعلومات. وقد ابتكر هذا الثنائي، وكان كلاهما يعمل في مركز الكومبيوتر العملاق في الجامعة، برنامج موزاييك، وهو أول متصفح ويب ضخم؛ وتتجلّى أهميته في أنَّه بات يتيح للناس الحصول على كل المعلومات الرائعة من «صفحات» الويب اليدوي بالضغط على الفأرة، بدلاً من الاضطرار لاستخدام أوامر قديمة وتناول حساء مثير للحيرة من مختلف حروف الهجاء والكلمات المركبة. وقد اكتسب هذا البرنامج فوراً صفة الظاهرة. وكان استخدام موزاييك يثير أشد الحماس بسبب المشاركة في تجربة ضخمة في مستقبل تبادل المعلومات. وسرعان ما أخرج فريق من المهتمين بجامعة إلينوي نسخاً من البرنامج تناسب كل منبر حسابي تقريباً. وأخذ ملايين الناس يتداولون هذه النسخ، وهبت آلاف المواقع على الشبكة لاستغلال هذا الجمهور.

في عام 1994 كان لأندريسين أن يتناول فنجاناً آخر من القهوة، ويكون له أثر، وشاركه فيه هذه المرة، رجل أعمال له استثمارات في سيليكون فالي هو جيم كلارك. وكان هذا المدير العام لشركة سيليكون جرافيكس، وقد غادر مكتبه ليحبث عن فكرة جديدة لشركة ناشئة، فوقع عند هذا الطالب الفتى على أحد أغنى المناجم في التاريخ. وكان كلارك الذي لم يكن محيطاً حتى ذلك الحين بفورة الشبكة، سريعاً إِلىٰ إدراك الإمكانات التجارية الكامنة فيها، فأمسك بأندريسين ذاته ومعظم فريق إلينوي ليطلق شركة موزاييك كميونيكا يشنس. (ولما اعترضت الجامعة على هذا الاسم استبدله كلارك بـ «نيتسكيب»

Netscape . وكان الغرض من هذه الشركة، تطوير نسخة محسّنة من المتصفح يدعى الجوال Navigator، مع برمجية بـ «مخدمات» الشبكة تسمح بإجراء الصفقات والمعاملات التجارية على الشبكة. وكان ثمة مكوّن ينقص هذا التصميم، هو الأمن. فإذا كانت الشركات تعتزم بيع منتجاتها وإجراء الصفقات التجارية على شبكة الإنترنيت فإن الزبائن سوف يطالبون بالتأكيد، بحماية سرِّيَّة مراسلاتهم. وهذا العمل المثالي للتشفير.

كان كلارك يعرف لحسن الحظ، شخصاً يعمل في هذا الحقل ـ جيم بيدزوس، فاتصل به؛ ولما انتهت المفاوضات بينهما، كانت نيتسكيب قد امتلكت ترخيصاً لاستخدام خوارزمية رسا والحصول على مساعدة الشركة في تطوير معيار للأمن لشبكة الويب: قاعدة تعتمد على مبدأ المفتاح العام تُعرف بـ «طبقة الممرات الآمنة» Secure Socket Layer. وقامت نيتسكيب بدمج هذه في برمجياتها، وهي تكفل للملايين من الذين تتوقع الشركة أنَّهم سوف يستخدمونها التمتع تلقائياً بمزايا التشفير كما تصوره ميركلي وديفي وهيلمان وقام على تنفيذه رايفست وشامير وأدليمان. فيكفي أن يضغط المرء على الفأرة ليدخل مستخدم نيتسكيب حالة التشفير، فتظهر على الشاشة رسالة تنبئ بأن المعلومات المسجلة كلها باتت في أمان. وفي غضون ذلك تكون عمليات التشفير والتثبت من هوية المرسل بطريقة الرسا جارية على قدم وساق.

كان جيم بيدزوس صلباً كعادته في المساومة مع نيتسكيب، وتم الاتفاق على أن تنال شركة الآر إس إيه مقابل الخوارزميات نسبة 1 بالمئة من الشركة الجديدة. وفي منتصف 1995، قدمت نيتسكيب أفضل عرض في تاريخ وول ستريت حتى اليوم، بحيث جعلت حصة الآر إس إيه من الشركة الجديدة تزيد عن 20 مليون دولار. (وجد بيدزوس العرض جيداً لشركة كانت قبل وهلة توشك على الانهيار، حتى تلقت 100 ألف دولار سلفة من لوتس).

كان ذلك بعيد عملية الإدخال والمعالجة والإخراج IPO التي أكسبت

العيون بصيرة، حين بدأ أحد زعران الشّيفرة يدعى هال فيني بالتدقيق في حال الأمان الذي تتمتع به نيتسكيب. وكان فيني، وهو مبرمج يعمل في سانتا برباره وله مساهمة في تطوير «منتهى السرِّيَّة» مهتماً بشكل خاص باستخدام الكريبتوجرافيا في التجارة الإلكترونية، وبات ملمّاً بـ «طبقة الممرات الآمنة». وقد طرحت نيتسكيب، نسختين من الجوال، التزاماً منها بأَنظمة التصدير: نسخة محلية ذات مفتاح من 128 بت لبرنامج آر سي ـ 4 المشفر ونسخة من 40 بت معدّة للتصدير.

ولقد طرح فيني على نفسه تحدياً يتمثَّل بتفكيك رسالة مشفَّرة بواسطة ذلك المفتاح الأضعف. فوضع مشروع صفقة نيتسكيب ـ كما لو كان عميلاً من العملاء ـ ثم استخدم التشفير في نسخة التصدير. ويقول في شرح التجربة: «ما قمت به أساساً هو الاتصال بالنيتسكيب وإحدى صفحاتها المأمونة وشرعت في طباعة بيان انتقيته عشوائياً وطلبت فيه قمصاناً رياضية أَو شيئاً من هذا القبيل». ثم التقط البيانات المشفَّرة وضمنها في تجربة التحدي:

التاريخ: الاثنين 10 تموز/ يوليو 1995 16 ـ 13: 52 ـ 700

من: هال < hfinney@shell.portal.com

إلى: < Cypherpunks@toad.com

الموضوع: لنحاول تحطيم المفتاح SSL RC4

لما تبين أن تفكيك برنامج مايكروسوفت أكسيس فاشل فيمكن أن يكون البديل محاولة تفكيك الـ 40 بت آر سي ـ 4، المستخدم في نظام نيتسكيب SSL طبقة الممرات الآمنة للتشفير المُعد للتصدير. . .

من بريطانيا، قبلت مجموعة آدم باك التحدي. ومع أنَّه كان يبدو أن خطة باك الأصلية، كانت توزيع مجال المفتاح بين عدة أشخاص، غير أنَّه انتهى إلىٰ قبول اقتراح مبمرج أوسترالي بالقيام بنصف بحث. أما بقية مجال المفتاح

فيتولاه متطوعون لكل واحد نصيب بجزء منه. ولقد نشب اضطراب بين الفئتين يومئذ مما أدّى إِلىٰ تباطؤ العمل بضعة أيام.

أثناء فترة تباطؤ العمل هذه، أخذ داميين دوليجه يتساءل عن سبب هذا البطء. كان دوليجه عالم كومبيوتر في السابعة والعشرين من العمر، وقد نال شهادة الدكتوراه قبل بضعة شهور ويعمل باحثاً لدى إينريا INRIA، مخبر الحواسب التابع للحكومة الفرنسية. كان مكتبه يقع في أحد الأكواخ في ما كان ذات يوم قاعدة للحلف الأطلسي على بُعد بضعة أميال من فيرساي. وكان له عناية شخصية بالتشفير، إذ بلغه شيء من النفور من الأساليب التي تلجأ إليها الحكومة قمع قابلية المواطنين للتواصل فيما بين بعضهم البعض، واعتقد أنَّه إذا استطاع أحدهم تفكيك إحدى منظومات التشفير ذات الأربعين 40 بت، التي أصبحت عرجاء بشكل مصطنع فسوف يكون ذلك ضربة بالقوة الغاشمة المهيمنة على المجتمع. كذلك ذهب به الظن إِلىٰ أنه بعد النجاح في تفكيك الخوارزمية رسا 129، سيكون بالإِمكان تنفيذ عمليَّة التفكيك في غضون أسبوعين أَو ثلاثة. لذلك أخذ يتساءل في خلده عن حقيقة ما حدث خلال الفترة ما بين التحدي الذي طرحه فيني وحل هذا التحدي.

كان لدوليجه القدرة على الوصول، بحكم عمله كباحث في مخبر الإينريا، إِلىٰ محطة العمل في مكتبه الصغير، وشبكة الكومبيوتر كلها، بما فيها الكومبيوتر ماسبار الضخم، أيضاً.

وكان هذا الباحث قد درس مواصفات طبقة الممرات الآمنة وطلع ببرنامج صغير يسمح للكومبيوتر اختبار المفتاح المحتمل بسرعة، ثم قام بتكييف البرنامج على نحو يجعله قابلاً للعمل في مختلف الآلات المتوفرة في شبكة اينريا، وبعض الآلات لدى الجامعات القريبة، ومعهد البوليتكنيك، وكلية الدراسات العليا.

ومن ثم بدأ بتنفيذ هجماته المتلاحقة. فكان كلما انحرف أحد العاملين

في إينريا عن كومبيوتره أو كومبيوترها ينبري برنامج دولجيه في غضون خمس دقائق، ويتناول ربما 10 آلاف مفتاح في ثانية. فكان يكفي المستخدم أن يلمس المفاتيح حتّى يستعيد سيطرته على الآلة. ولم يكن هناك من شكوى.

ولقد حسب دوليجه، أن فرصته ستكون أفضل في العثور على المفتاح، إن بدأ من نهاية مدى المفتاح ورجوعاً إِلىٰ الأمام: «لقد اعتقدت أن زعران الشّيفرة يبدأون من البداية، فبدأت أنا من النهاية». فجهز شبكته للعمل في يوم الجمعة المصادف 4 آب/ أغسطس، وغادر مكتبه لقضاء عطلة نهاية الأسبوع. ولما عاد يوم الاثنين ليستأنف العمل اكتشف خطأ في برنامجه. فعاد يجدد العمليّة من البداية. وكان أن أخذت عمليّة معالجة الأعداد تجري على أحسن ما يرام، منذ تلك النقطة، إِلاّ أن الأمر انتهى بدوليجه إِلىٰ عشر نسخ جديدة من البرمجيات، خلال الأيام القليلة لمعالجة ذلك الخطأ في الاتّصالات بين الآلتين. كان البرنامج يجري على ما يرام حين غادر دوليجه عمله يوم الجمعة 11 آب/ أغسطس وكانت العطلة الأسبوعية تمتد هذه المرة، بسبب مصادفتها مناسبة منتصف الصيف الذي تحتفل به فرنسا كلها، أربعة أيام فتنتهي في 15 آب/ أغسطس. ولكنّه حين تفقد كومبيوتره الخاص في البيت، قبل انتهاء العطلة الانتصافية وجد برنامجه يقدم له رسالة كان ينتظرها.

قال: «وجدت أن الكومبيوتر قد عثر على المفتاح». وإذن فقد تم تفكيك طبقة الممرات الآمنة!

وفي اليوم التالي قاد دامبين دوليجه سيارته من منزله خارج باريس عائداً إِلىٰ عمله، واستعاد هناك المفتاح من محطة العمل، ثم التفت إِلىٰ تفكيك الرسالة على أكمل وجه. فلما تم له ذلك وجّه رسالة إِلىٰ زعران الشّيفرة، وكانت تحمل العنوان التالي: «تحدي طبقة الممرات الآمنة: فُكك». وللبرهان على ذلك أرفق رسالته بالنص الواضح الصريح للرسالة المشفَّرة. ولقد قدر أولئك الذين يعرفون الرسا 129 أهمية عنوان الشخصية الخيالية التي ابتدعها هال

فيني في رسالته المشفرة: السيد كوزميك كومكوات، شركة طبقة القوابس الآمنة المساهمة، يقيم في 1234 (شارع صقر السمك المتقزز).

وبالرغم من أن فكرة تفكيك شيفرة نيتسكيب، ليس فيه من الناحية الفنية ما يصدم المرء، إذ تفرض رياضيات التشفير، أن يتهاوى المفتاح الضعيف حين يتعرّض لهجوم مركّز، فإنّها استولت على مخيلة الصحافة الشعبية. وأصبح دوليجه هدف وسائل الإعلام. ولأن هذا الخرق جرى بعد أسبوع واحد من الفوز المؤزر الذي حظيت به نيتسكيب ولعله كان أعظم نجاح تحقّق في التاريخ في عملية إدخال وإخراج ومعالجة. فقد أبرز بعض الصحفيين هذا الخرق وكأنما يمس أمن المتصفح كله، وليس باعتباره مثالاً على أثر أَنظمة التصدير التي تأخذ بها الحكومة في إضعاف البرمجيات على العموم. وقد لاحظت نيتسكيب في رسالة بثتها عبر موقعها في وقت لاحق من الأسبوع أن دوليجه إنما استطاع تفكيك رسالة واحدة وحسب، واستغرق في ذلك (MIPS 64 عاماً) أي توجيه 64 مليون أمر في الثانية من السنين، وقدرت تكاليف عمليّة التفكيك 10 آلاف دولار. ولكن دوليجه نفّذ العمليّة كما قال في أوقات العطلة والراحة ودون أن يتكبّد أية نفقة. غير أن موقف نيتسكيب كان أرسخ حين لاحظت أن النسخة المباعة في الأسواق المحلية من برنامج المتصفح الجوال Navigator اعتمد على مفتاح أفضل يتكون من 128 بت؛ وقالت في رسالتها: «يجب أن يكون الكومبيوتر اللازم لتفكيك مثل هذه الرسالة، بتريليون تريليون ضعف قوة الكومبيوتر المستخدم في فكّ شيفرة الرسالة آر سي ـ 4 ـ 40».

وكانت هذه النقطة عينها، هي جوهر الأمر عند زعران الشّيفرة: وهو أن برامج التفكيك المعدّة للتصدير ضعيفة دونما مبرّر.

ولكن زعران الشّيفرة لم يكونوا قد أنهوا الأمر ونيتسكيب. ففي بيركلي، وجدنا اثنين من طلبة الدراسات العليا يتحولان إلىٰ تحليل الشيفرة، وهما إيان جولدبرج وديف واجنر، وكلاهما في الثانية والعشرين من العمر، وقد وجد

هذان، ما يحملهما على التطفّل على النيتسكيب، أي سفينة القيادة في أمن الإنترنيت. وكان كلاهما قد قصر عن الهجمات بالقوة الغاشمة، كان جولدبرج قد انتقل حديثاً من موطنه كندا إِلىٰ كاليفورنيا بينما كان واجنر قد قدم لتوه بعد نيله إجازته الجامعية من جامعة برنستون. وهكذا أخذ الاثنان يختبران شكلاً مختلفاً من الهجوم، وكان أقرب للتوصية الثانية التي أوردها روبرت موريس: ابحث عن النص الأصلي الصريح. فهل يحتمل أن يكون فريق الأمان في نيتسكيب قد ارتكب خطأ بسيطاً، ولكنّه فاحش، في تنفيذ برنامجهم، مما يكشف للمتنصتين ما قد يبلغ ملايين الصفقات التجارية التي تتم عبر الأَجهزة الإِلكترونية؟ إن ذلك مستبعد. ولكن المرء، كما ألمح موريس، يظل جاهلاً إِلىٰ أن يبحث من حوله حتّى ينجلي له الأمر.

وهاكم متى رأى واجنر السر. فقد وجد الرجل أن التعليمات لمولد الأعداد العشوائية، مدفونة في رموز النيتسكيب وهذا جزء هام من أي نظام تشفير راقي. الجزء الحاسم في التشفير لتعمية الرسائل الذي يجعل النص المشفر خلواً من الإشارات التي تنم عن نمط معين يرشد محلِّل الشيفرة إِلىٰ ثغرة في الرسالة. فمن المعلوم تماماً أن افتقار العشوائية الحقّة ضعف يستطيع محلِّل الشّيفرة استثماره متى وقع عليه. لذلك كان من الضرورة بمكان توفّر مولد أعداد عشوائية متين، بحيث يجعل دولاب روليت حروف الهجاء يدور على أفضل ما يكون الدوران. كذلك ثمة جزء هام في مولد الأعداد العشوائية يتجلّى في استخدام «بذرة» غير متوقعة، وهي عدد تبدأ به العمليَّة العشوائية. فلما كانت الكومبيوتر تجري مجراها ذاته كلما تحرّكت ـ وهي في ذلك عكس النرد ـ فإنّه من الضروري أن تبدأ ببذرة لا يملك الخصم المحتمل أن يحدس ماهيتها بأي حال. وغالباً ما تشتمل أساليب تنفيذ هذا استخدام إحصائيات غريبة غير مألوفة من عالم الواقع ـ وضع الفأرة مثلاً، أَو أي أمر لا يمكن لعدو معرفته.

أما نيتسكيب فقد أهملت، كما تبين، هذه الحكمة. فما أن دقّق ديف واجنر النظر في الشّيفرة، حتّى برز له الخطأ. والسر في ذلك أن نيتسكيب استمدت بذرة مولد الأعداد العشوائيّة من ثلاثة عناصر: الوقت المدون في الرسالة وشكلين في تعريف المستخدم يعرف الأول باسم هوية العمليّة وهوية الأم. وتلكم هي الكارثة. ذلك أنه يكفي الخصم أن يدير الكومبيوتر بضعة دورات ويشغل عدداً من خلايا الدماغ أقل من دورات الكومبيوتر ليعثر على القسم الأول من البذرة: فمن اليسير على المرء أن يعرف العدد المحدود من أوقات اليوم. وغالباً ما يكون من اليسير على المرء العثور على أرقام التعريف، في كلتا الحالتين، خاصة إذا كان ثمة من يشترك مع آخرين في المخدم ذاته، كما هو الحال غالباً في بيئة مثل الإنترنيت. يقول جولدبرج: إذا كان للمهاجم سجل للآلة التي لديك، غدا الأمر بسيطاً. ولدينا هنا في جامعة بيركلي آلاف المستخدمين. فإذا كان هناك من يستخدم النيتسكيب، استطاع اكتشاف الهويتين». غير أنه بوسعك اكتشاف هاتين الهويتين ببساطة، وإن لم تتوفر لك هذه الميزة. وجدير بالذكر أن أرقام الهويتين المطلوبتين لا يزيد طولهما عن خمسة عشر بت، وهذا رقم يسهل مهاجمته بالقوة الغاشمة.

ولقد أمضى واجنر وجولدبرج العطلة الأسبوعية في وضع برنامج لاستغلال هذا الضعف، ولما كانت ليلة الأحد جلسا لامتحانه، واستطاعا اكتشاف المفتاح السري في أقل من دقيقة، بالتركيز على الثغرة الضخمة في برنامج النيتسكيب. ووداعاً لأمن الشبكة، وبعث جولدبرج بالنتيجة إلىٰ قائمة زعران الشّيفرة. وقال معلّقاً: لم نكن نتوقع أن تحظى هذه الواقعة بكثير من العناية من الصحافة. ويا لسذاجة الفتى. لقد كان بين قراء تلك الرسالة مخبر في صحيفة النيويورك تايمز، فقام هذا بنشر الخبر. فلما ظهر في صحيفة الوقائع أخذ الفضوليون والصحفيون يتقاطرون على هذين الطالبين، وهما لما ينالا شهادة التخرّج بعد. وكان من بين ما صرح به هذان الطالبان، تلك الملاحظة

التي أدلى بها جولدبرج، وتحمل على التفكير: «إننا شابان طيبان، ولكننا لا ندري إن كان هناك من الأشرار من وقع على هذه الثغرة مثلما وقعنا نحن عليها».

كانت هذه سقطة شنيعة، على العكس من عمليَّة فك الشّيفرة الأولى على النيتسكيب، حيث كان يمكن لهما القول أن رسالتهما المشفرة كانت على قدر عظيم من المنعة لولا القيود التي فرضتها الحكومة. ذلك أنك لم تكن بحاجة هذه المرة إِلىٰ رصد شبكة مؤلفة من عدد كبير من المحطات، أَو الوصول إِلىٰ كومبيوتر ضخم لتتمكّن من حل الشّيفرة. فهناك حالات معينة لا تحتاج فيها إِلاَّ لدقيقة واحدة من متعة معالجة الأَرقام. قال مايك هومر، نائب رئيس نيتسكيب لشؤون التسويق: «إن المهندسين لدينا ارتكبوا خطأً في تنفيذ البرنامج».

ولقد أرخى هذا الخطأ ظلالاً من الشك، حول مبلغ الأمان، الذي توفره شركة برمجيات الإنترنيت الرائدة. وقد حمل هذا عالم الشيفرة بروس شتاينر على التساؤل: «إذا كانت نيتسكيب قد ارتكبت هذا الخطأ، فقد تكون هناك أخطاء أخرى أيضاً». ولكن السؤال الملحّ الذي يحتاج إِلىٰ إجابة هو إن لم تكن نيتسكيب مأمونة، فأين الأمان إذن؟ والسبب في السؤال هو أن نيتسكيب كانت تبذل قصارى جهدها لحماية مستخدِميها. وإذا كان يمكن اختراق برنامج الجوال بهذا القدر من اليسر، فأي أمل هناك إذن للآخرين بالفلاح؟

لكن لتلك الواقعة جانبها المشرق أيضاً: فبوسعك أن تذهب مذهب القول أن الأمور سارت على الوجه الأفضل، لأن زعران الشّيفرة كشفوا ضعفاً في النِّظام واضحاً فعمدت نيتسكيب إِلىٰ تلافيه فوراً. لكن الدرس الذي رسخ كان أشد قتامة إِلىٰ حد ما. فمع انتشار الإنترنيت أخذ الجمهور يعتمد حقاً على الكومبيوتر المرتبطة ببعضها في عقد الصفقات التجارية وتخزين المعلومات، بدءاً من شراء الكتب فشراء وبيع الأسهم إِلىٰ تسديد الفواتير. وشرعت مصالح تجارية تخطط، لعرض السجلات التجارية على شاشات شبكات الكومبيوتر.

ولكن الأمان ظل، في أحسن الأحوال، مقلقلاً. وكان ثمة سبب عظيم واحد يزداد جلاء باطراد فيه تفسير هذا القصور، وهو العرقلة المستمرة من جانب حكومة الولايات المتّحدة. وفي حين حاولت الحكومة الترويج للمقراض ووديعة المفتاح كحل مفضل للمشكلة، ظلت الإنترنيت تحث الخطى ـ دون جهد منظم لتوفير ما تحتاج إليه من أسباب الحماية.

في منتصف التسعينات وجد أولئك الذين كانوا يجهدون لبلوغ عصر جديد من حماية الشّيفرة عصر يوفر الأمان للإنترنيت ووسائط الاتّصالات الإلكترونية الأخرى أنفسهم تحت وابل متزايد من النيران. وبدا أن أولئك المسؤولين عن القوانين والمؤسسات الاجتماعية كانوا قادرين على فعل الكثير، لحمل المجددين في التشفير على إدراك أن لأفعالهم عواقب، وإن عجز المسؤولون هؤلاء عن قطع أسباب التقدم أمام الرياضيات والهندسة. وأصبح السؤال عندئذ إلىٰ أي حد يمكن للحكومة، أن تمضي في تهديدها بهذه العواقب.

بالنسبة لراي أوزي، في شركة لوتس، لم يكن تلقي مثل هذا الدرس في قدرة السلطة بالأمر اللازم، فقد كان الرجل ملتزماً بالعمل في إطار النظام القائم. (فضلاً عن ذلك كانت لوتس قد انضمت إلىٰ المؤسسة رسمياً، في عام 1993، حين قامت شركة الآي بي إم بشرائها، بمبلغ ثلاثة بلايين دولار). وكان أوزي قد أصبح في السنوات التالية لتبنيه المبكر لخوارزمية رسا، شخصية ذات صوت مسموع في معارك التشفير، في شهاداته أمام الكونجرس والزيارات التي كان يقوم بها للشخصيات البارزة في الحكومة. ومع أنّه كان واضحاً في انحيازه إلىٰ التشفير إلاً أن ما كان يتحلى به من كياسة واستعداد للأخذ بالرأي المعارض بعين الاعتبار أكسباه احترام حتّى المتشددين في موضوع التصدير. وقد دأب الرجل، وهو غير قادر على انتظار

الحكومة لتحرير قوانينها، على البحث عن طُرق جديدة لتجاوز العقبات التي تضعها أَنظمة التصدير وتعرقل التجارة.

بعيد تفكيك رسالة نيتسكيب، أخذ زبائن لوتس نوتس يزدادون ضيقاً باستخدام برنامج التشفير بـ 40 بيت من آي بي إم المسوح بتصديره إلىٰ الخارج. وكانوا يريدون معرفة السبب في بيع الزبائن الأمريكيين نسخة ذات مفاتيح مكونة من 64 بت، وهي بملايين المرات أصعب من النسخة المصدرة إليهم التي يمكن تفكيكها على يد حامل شهادة دكتوراه وقعت بيده على غير اتفاق هذه الرسالة في ضاحية من ضواحي باريس. (وفي تلك الأثناء كانت الشركات التي لم تشأ، مثل مايكروسوفت، أن تقدِّم المُنتَج ذاته بنكهتين، تقدم لزبائنها كافة برنامج التشفير الأضعف. وقد أدَّى هذا العقيم إلىٰ خفض قيمة خط الإنتاج كله عند أولئك الذين ينشدون التشفير، فالتفت بعض هؤلاء الزبائن إلىٰ الشركات الأجنبية، التي تستطيع بيعهم برنامج التشفير الأقوى بصورة قانونية).

في عام 1995 طلع أوزي بما بدا أنه تسوية مقبولة، على الأقل في المدى القصير: وكانت هذه تقوم على حيلة رياضية لتلبية متطلبات وكالة الأَمن القومي. وتتضمن خطة أوزي، نسخة أزهد ثمناً من المقراض، على ما كان عليه من النفور منه، ومع ذلك فقد ظلّت لوتس تبيع نسختين من النوتس، إنما تختلفان عن النسخ الأخرى من حيث أنهما ببرنامج تشفير من 64 بت. غير أن النسخة الدولية تحمل معها هدية صغيرة لوكالة الأَمن القومي: مجال دخول الأَمن القومي NSAF، ويتألَّف من 24 بت من البيانات المشفَّرة التي لا يملك تفكيكها سوى وكالة الأَمن القومي وحدها. وكان هذا البرنامج مشفراً بالمفتاح العام للوكالة، بحيث لا يستطيع تفكيك ذلك المجال إلاَّ أهل «القلعة» حصراً. وجدير بالذكر أن الرسائل المشفَّرة وفق برنامج النوتس يتقلص، بعد استخدام وكالة الأَمن القومي مفتاحها الخاص، لتفكيك برنامج مجال دخول الأمن

القومي ذي الـ 24 بت، من نص مشفَّر من 64 بت، إلىٰ نص مشفر آخر من 40 بت. وكان تفكيك الشّيفرة المتبقية تتطلب القدر من العمل ذاته الذي تتطلبه الرسائل المشفَّرة بمفاتيح بطول 40 بت المصدرة مع النِّظام القديم. ولكن بما أن التشفير كان على وجه الإجمال أقوى من قدرات المهاجمين جميعاً، عدا وكالة الأَمن القومي ـ وكان مصدر القلق لدى معظم المستخدمين المهاجمين الآخرين، كالمخبرين وجواسيس الصناعة ـ فقد اعتقد أوزي أن هذا الحل ربما كان مفيداً في المدى القصير.

ولقد تقدمت لوتس بطلب براءتين لابتكارها هذا، وعرفته باسم «نظام وطريقة شيفرة عامل التشغيل التفاضلي» في كانون الأول/ ديسمبر 1995 وأدمجته في النسخة الجديدة من برنامجها نوتس ـ الإصدار 4 Notes Release 4. وكان أول حديث أدلى به أوزي عنه علناً في كانون الثاني/ يناير 1996، في مؤتمر لشركة آر إس إيه داتا سيكيوريتي، في سان فرانسيسكو. وكان هذا المؤتمر أحد المناسبات التي يقيمها جيم بيدزوس لعرض الأفكار الجديدة في التسويق. فقد دأبت إِدارة الشركة منذ 1990 على جمع زبائن الشّيفرة التجارية في منطقة خليج سان فرانسيسكو، في إطار ندوات ومعرض صغير يستعرض فيه البائعون بضائعهم على مدى بضعة أيام. وكان هذا المؤتمر قد بدأ كاجتماع يضم قلة من السحرة والحواة في فندق سوفيتل بالقرب من مكاتب الشركة في رد وود سيتي ثم تطور إِلىٰ حشد من عدة آلاف وبات يعقد الآن في فندق ضخم بالقرب من ساحة يونيون سكوير. وقد حازت كلمة أوزي على اهتمام واسع كما أثار بين المستمعين قدراً من الضيق، وحمل البعض على التساؤل، إن كان المصمّم المبتكر خلف برمجيات النوتس قد تخلّى عن الكفاح واستسلم.

لا، إنه لم يستسلم؛ بل كل ما في الأمر أنّه كان منشغلاً بمتابعة جدول أعمال، أكثر دقة مما يشغل الآخرين، وعبَّر عن ذلك بقوله: «لقد كنت أسعى

إِلىٰ تحريك الأمور». وكان هدفه يومذاك، أن يضرب إسفيناً بين الإِدارة ووكالة الأَمن القومي. وقد ذهب به الفكر يومذاك مذهب أنه متى تراجع آل جور عن فكرة سيطرة الحكومة على ترتيبات الإيداع فلن تجد وكالة الأَمن القومي مسوغاً عظيماً لأفكار ما بعد المقراض. ذلك أنه إذا أخذ الناس، بإيداع المفاتيح في مستودعات خاصة فسوف تضطر السلطات عندئذ إِلىٰ الحصول على أمر قضائي حتَّى تستطيع وضع يدها على هذه المفاتيح. وفي هذا ما يضر بأسلوب عمل الوكالة، فهل تعمل بالسر ويحظر عليها رصد ما يجري داخل البلاد. وبالتالي فإن الخطة التي اقترحها أوزي تنطوي على شيء من الإغراء، من حيث أنها تسمح لها بأن تحقِّق قصب السبق في عمليَّة تحليل الشَيفرة. (ذلك أنَّها لن تحتاج في هذه الحالة إِلىٰ أمر قضائي للحصول على مفتاح فك شيفرة من 24 بت). وإذن فقد كانت خطة أوزي بعيدة كل البُعد عن خذلان دعاة التشفير، بل هي استراتيجية تخريب لدفع وكالة الأَمن القومي والإِدارة إِلىٰ الاختلاف حول طُرق معالجة متعارضة. وقد أمل أوزي بأن تفيد الصناعة من حالة فوضى الآراء لتنفذ حلها الخاص.

ولكن أوزي اكتشف، قبل أن يهنئ نفسه لحصافته، أن الحكومة لم تكن لتفتقر إِلىٰ وسائلها الخاصة للتعامل مع أمثال هذه الاستراتيجيات. ففي 30 كانون الأول/ ديسمبر 1996 تلقى أوزي وشريكه المخترع تشارلز كاوفمان رسالتين وعلى الغلاف عبارة «أمر سرِّي». وأفادت الرسالتان أن طلبيهما المتعلقين ببراءة الملكية الفكرية «يتضمنان موضوعاً قد يؤدي الكشف عنه دون تصريح، في رأي الجهة المعنية في وزارة الدفاع إِلىٰ ضرر فادح ينال من الأمن القومي»: (لوحظ في الفراغ المتروك لإشارة المسؤول الحكومي عن براءة الملكية الفكرية علامة X إِلىٰ جانب كلمة «الجيش»). وقد حذَّرت الرسالة من أن الكشف عن موضوع الطلب دونما تصريح لأية جهة يجعل المخترعين، وشركة آي بي إم، عرضة للعقوبات التي تشمل السجن. وفي النهاية أعلم

الرجلان بأنّه يتوجب عليهما إتلاف النسخ موضوع الطلب، على النحو الذي يمنع الكشف عن محتويات الوثيقة أو الإفادة منها».

أدرك أوزي، فور تلقي الأمر يوم 7 كانون الثاني/ يناير 1996، أن الامتثال للأمر ينطوي على مشكلة. فهو قد سبق له أن خاض في تفاصيل المشروع في عدة مناسبات، كما تم توزيعه فعلاً على حوالى ستة ملايين شخص يستخدمون برنامج اللوتس نوتس، نصفهم خارج الولايات المتّحدة. فأسرع إِلىٰ إخطار رؤسائه في الشركة بما بلغه، وأخذ هؤلاء في التفكير بالعواقب المترتبة على اعتبار أحد أكثر برمجياتهم شعبية في العالم سراً من أسرار الحكومة.

ولعل أفضل ما قام به أوزي أنه دفع بصديق له للاتّصال بنائب مدير وكالة الأَمن القومي بيل كرويل، الذي ضحك كما ذكر، حين سمع بالخبر وقال للصديق أنه سوف ينظر في الأمر. وفي 9 كانون الثاني/ يناير اتصل كرويل بأوزي، وقال له أن في لأمر خطأ وسوف يصار إِلىٰ إصلاحه. وبالفعل أُخبر محامو شركة آي بي إم حين اتصلوا بمكتب براءات الملكية الفكرية بأن الأمر السري قد طوي، ثم ورد كتاب بالفاكس بهذا المعنى يؤكد الكلام الشفهي الذي بلغهم أثناء المكالمة الهاتفية. وهكذا لم يعد راي أوزي وشريكه المخترع وآي بي إم معرضين للمقاضاة عن ستة ملايين مخالفة لقانون سرية براءات الاختراع. ولكن بعد أن تنفس الجميع الصعداء وجدوا الأمور ما تزال على حالها. فإذا كان هذا المآل الذي ينتهي إليه من يعمل على خدمة زبائنه بروح وديعة المفتاح، فما هو مصير أولئك الذين يتصدون للحكومة صراحة؟

لقد كان جواب هذا السؤال عند جيم بيدزوس. ففي الوقت الذي اتخذ فيه أصرح موقف علني في معارضة الحكومة ـ فقد ذهب به الأمر إِلىٰ حد توزيع ملصقات تحث الشعب على «إغراق المقراض» كانت العلاقة بين شركته ووكالة الأَمن القومي تتدهور باطراد. وبالرغم من أنَّه لم يكن لديه أي دليل مادي على أن هاتفه كان يخضع للمراقبة فقد حسب بأنه تحت المراقبة.

ولعل أشنع المواجهات كانت ما حدث في نيسان/ أبريل 1994، أثناء اجتماع مع ثلاثة من المسؤولين عن قضايا التصدير في وكالة الأَمن القومي، وكان لبيدزوس معهم جميعاً صراع منذ سنوات. وكان من هؤلاء الثلاثة امرأتان له بهما قدر من الثقة، أما الثالث فكان رجلاً ينطوي على مقت لا ريب فيه لبيدزوس وشركته.

ولما وجد بيدزوس، فريق وكالة الأَمن القومي لا يطرح أية قضايا محددة لفتح باب التفاوض معهم، استغل المناسبة ليحاضر فيهم في موضوع المقراض، فقال أنه لن يجد من يقبل عليه، ووصفه بالنِّظام الحافل بالعيوب وإلخ. ولاحظ بيدزوس أن الرجل بين جماعة وكالة الأَمن القومي، بدأ يزداد ضيقاً بحديثه. ثم تكلم في النهاية، وخاطب بيدزوس قائلاً: إن صادفتك في ساحة وقوف السيارات فلن أتردد في دهس مؤخرتك حتَّى تستوي مع الأرض.

ويذكر بيدزوس أنه صعق لما سمع، لكنَّه قال في النهاية مخاطباً الرجل: «سوف أمنحك فرصة لسحب كلامك أَو الاعتذار. ولكن هذا استمر في الضغط وصاح هائجاً: «إني جاد في ما قلت. لكنك لم تستوعب ما قلت، أَمْ لعلك استوعبت الكلام؟»».

هل كان بيدزوس يتلقى تحذيراً رسمياً، ما يعادل قبلة المافيا على الشفتين من السياج الثلاثي؟ هل يجب عليه أن يتجنّب ساحات وقوف السيارات؟ لقد خالجه شعور بأن الرجل كان ينفث عن غضبه وحسب، إلاَّ أنه لم يشأ أن يدع التهديد يمضي دون رد. فأخبر أحد الصحفيين بما كان، وإذ بالقصة تظهر في إحدى الصحف المحلية. ثم لم يمض إلاَّ وقت قصير حتَّى تلقى مكالمة من رئيس ذلكِ الموظف في وكالة الأَمن القومي يعتذر فيها عن تلك الحادثة. ولقد راود بيدزوس شعور بأن الوكالة تريد منه ترك العمل، وإن لم تكن حياته في خطر.

ولكن بيدزوس شعر بالارتياح مع ذلك، إذ لم يعد تحت وطأة التهديد

بالمقاضاة. فهذا المصير كان محفوظاً للرجل، الذي نغص عليه حياته ذات يوم، فيل زيمرمان. كان زيمرمان يحسب منذ نشر برنامجه «منتهى السرِّيَّة» أن مشكلته الكبرى تكمن في الخلاف مع شركة آر إس إيه بشأن حق الملكية الفكرية. لكن جيم بيدزوس لم يكن بالمقابل ليجد مشقة في مهاجمة زيمرمان علناً. كان حسبه أن يضغط زر جهاز الفاكس فيتلقى الصحفيون نسخة من تعهد زيمرمان المكتوب (بصيغة غامضة) بإيقاف توزيع البرنامج، وهو تعهد يبدو أنه لم يلتزم بروحه. غير أنه لم يكن ليراود زيمرمان خاطر بأن يجد نفسه عرضة للتحقيق النائي. وهكذا حسب عندما جاءته امرأتان من دائرة الجمارك الأمريكية في شمال كاليفورنيا في 1993، أن سبب الزيارة دعوى من جيم بيدزوس. والحق أن هاتين المفتشتين تناولتا موضوع توزيع البرنامج وكيف كان يتم، إلاَّ أن معظم الأسئلة كانت تنصب على التشابه بين برنامج «منتهى السرِّيَّة» ومُنتَجات شركة آر إس إيه. وكان واضحاً للعيان أن المفتشتين كانتا تفتقران للخبرة في المسائل التكنولوجية. فكان على زيمرمان أن يشرح لهما الأفكار الأساسيَّة التي يقوم عليها التشفير وتوزيع البرمجيات. ولما غادرت المفتشتان المكتب كان الرجل مطمئناً إلىٰ أن الموضوع طوي، ولم يعد لديه إلاَّ القليل مما يشغل باله. وحدثته نفسه أن الحادثة كانت مضايقة له من بيدزوس، وقال يومئذ: «لا أعتقد أنهم هناك سيتخذون أي إجراء ضدي. لقد أثارت المفتشتان بعض الأسئلة حول [أَنظمة التصدير]، ولكني تمكنت من إنهاء هذا الموضوع».

وكان ذلك صحيحاً، إنما ليس تماماً. فقد كان يراود المدعي العام في الولايات المتّحدة وليم كين خشية من أن يكون قد جرى خرق أَنظمة التصدير. وكان لذلك الخوف ما يبرّره، إذ لم يكن قد مضى إلاَّ ساعات على نشر برنامج «منتهى السرِّيَّة» على الإنترنيت حتى كان هذا البرنامج القوي قد وجد طريقه إلىٰ خارج الولايات المتّحدة. وليس واضحاً ما إذا كانت واشنطن قد مارست ضغطاً إلاَّ أن الواقع هو أن كين أخبر زيمرمان بعد بضعة أسابيع من تلك الواقعة بأنَّه

سيخضع للتحقيق بتهمة تصدير ذخائر حربية إِلىٰ الخارج. (كذلك استهدف التحقيق كيلي جوين الذي عرف نفسه للصحفي جيم وارين الذي يعمل في مايكرو تايمز على أنَّه جوني آبلسيد في «برنامج منتهى السرِّيَّة»).

ولقد ظل زيمرمان، يعاني طوال السنوات الثلاث التالية من جحيم قانوني، يحقق في أمره هيئة من المحلفين، إنما دون إدانة. ونصحه محاموه بالابتعاد عن الأضواء. غير أن الشهرة التي أصابها برنامج «منتهى السرِّيَّة» أكسبت فيل زيمرمان ميلاً للحديث والتعبير عن آرائه بصوت عالٍ. وفضلاً عن ذلك كان يرى أن فرصته الكبرى في طرح الموضوع علناً أمام الجمهور. وكان يجد أن الناس العاديين كانوا يثورون كلما حدَّثهم عن برنامج «منتهى السرِّيَّة» والموضوعات التي تتصل بالتشفير، ويتصاعد غضبهم من احتمال قيام الحكومة بالحد من إمكانية التواصل في ما بينهم دون تدخّل من أحد بهذه الحرية والخصوصيَّة. ولقد ظن ولسبب وجيه أنَّه حتى الذين لا خبرة لهم بالتكنولوجيا سوف يضيقون بهذه الفظاعة الجديدة، حيث الأخ الكبير ذاته يعد غرفة في السجن لمن يقوم بتوزيع برمجيات توفر الخصوصية للمقاتلين من أجل الحرية والعشاق وأوئك يرون أنه لا شأن لأحد بأسرارهم. والأكثر من ذلك أن التهمة الموجهة إِلىٰ زيمرمان كانت ضعيفة لا تصمد عند الامتحان؛ فالرجل لم يكن مرسل البرنامج إِلىٰ الشبكة. والشخص الذي قام بذلك أخبر [الصحفي] جيم وارين، بأنَّه كان شديد الحرص على اقتصار عمليَّة التوزيع على المواقع الأمريكية وحسب. فهل كانت وزارة العدل تؤكد في واقع الأمر على أن القيود التي تنص عليها أَنظمة التصدير تحظر على المواطنين الأمريكيين، توزيع مواد مباحة قانونياً على مواطنين أمريكيين آخرين؟

وآه من أَنظمة التصدير. إنك كلما أطلت النظر فيها، وجدتها تبدو أشد غرابة من ذي قبل، ومن القضايا المثيرة مؤخرا قضية تتصل بكتاب «الكريبتوجرافيا التطبيقيَّة» لمؤلّفه بروس شتاينر والصادر عام 1994. وكان الكتاب

مرجعاً شاملاً لنظرية الشيفرة الرياضية، ويضم شروحاً لمنظومات التشفير الشائعة وكافة الخوارزميات التي قد يحتاج إليها كل مختص بالأمن أَو زعران الشّيفرة. وقد عرفه كتاب The Millenium Whole Earth Cataloge بأنَّه «الكتاب المقدس لهواة الشيفرة». والمفارقة في الأمر أنَّه يمكن لأي شخص أن يصدر الكتاب برمته إِلىٰ مختلف أرجاء العالم، سوى أن القيود المفروضة في موضوع التشفير تحظر على ما يبدو تصدير محتوياته بشكل رقمي. هذا على الأقل ما اكتشفه فيل كان، أحد زعران الشّيفرة، حين طلب الإذن بتصدير الكتاب وفق الصيغة الرسمية CJ Commodities Jurisdiction مع القرص المرن الذي يرافق الكتاب ويضم نفس محتوياته. ولقد وافق المسؤولون على تصدير الكتاب ذاته إنما دون القرص المرن. وبدا الأمر عندئذ سخيفاً.

وأخذ زيمرمان يتحدَّث ويثير ضجيجاً من حوله. وكان كثيراً ما يذكر في أحاديثه أن الثوار في بورما على ما تشير التقارير يستخدمون برنامج «منتهى السرِّيَّة» للتستر على نشاطاتهم المعادية للحكومة؛ وقد ذكر في شهادة له في جلسة استماع أمام إحدى لجان الكونغرس سنة 1993 أنه تلقَّى شكراً من وطني من لاتفيا وزعم: أن «برنامجك منتهى السرِّيَّة شائع ومستخدم من بحر البلطيق حتى الشرق الأقصى وكفيل بمساعدة الشعب الديمقراطي عند اللزوم». ولما اتهمته الدوائر الأمنية بأن برنامج «منتهى السرِّيَّة» يفيد منه المجرمون على وجه الخصوص، وقد استند هذا القول إِلىٰ واقعة في سكرامينتو، حين تعذّر على رجال الشرطة قراءة يوميات أحد مرضى الشذوذ الجنسي المشفَّرة، وفق برنامج زيمرمان، أجاب أن للتكنولوجيا فوائد ومضار.

ولعل الواقعة التالية تبين مدى الشهرة التي أصابها زيمرمان؛ اصطحبه بعض رجال الأعمال ذات ليلة لقضاء سهرة في سان فرانسيسكو، حتى انتهى بهم المطاف في ناد بنورث بيتش يعرض برنامجاً تتعرَّى فيه الراقصات. وقد

سألته إحدى الراقصات حين أصبحت بالقرب منه عن عمله. فأجابها: «إنني أعمل بالتشفير، وقد وضعت برنامجاً اسمه منتهى السرِّيَّة».

توقفت الراقصة عن هزّ وسطها، وسألته كالمذهولة: «أأنت فيل زيمرمان؟ إني أعرف «منتهى السرِّيَّة» وكل ما يتعلَّق به جيداً».

حقاً إن المرء لا يصادف مهووسين بالشّيفرة، ويعملون في مجال الجنس، كل يوم. ولكن الحق أيضاً، أن روّاد برنامج منتهى السرِّيَّة كانوا قد أخذوا يتجاوزون نطاق المجانين والمهووسين بالسرِّيَّة. وقد ذكرت صحيفة وول ستريت جورنال أن المحامين يستخدمون هذا البرنامج للحفاظ على سرِّيَّة المعلومات والكتَّاب لحماية الأعمال التي هي قيد الإنجاز حفاظاً على حقوقهم الأدبية كما يستخدمه عالم فلك في تسجيل اكتشافاته.

وليكسب رجال الأعمال والفعاليات التجارية عمد زيمرمان إلىٰ منح شركة تدعى فياكريبت، حق إنتاج الشيفرة، ولما كانت الشركة المذكورة تدفع أجراً لشركة آر إس إيه لقاء حق استخدام مُنتَجها، فيمكنها إذن أن تبيع برنامج منتهى السرِّيَّة لزبائنها من رجال الأعمال دون أن تخشى المقاضاة. (اعتقاداً منها أن ليس في دفع أجرين لقاء استخدام البرامج ما يضير، بفضل تميز برنامج منتهى السرِّيَّة كمُنتَج رائع والإقبال الواسع الذي يحظى به من الرواد غير الظاهرين).

وبدءاً من 1994 أصبح لنقطة التوزيع الرئيسة، للنسخة المجانية الأكثر شعبية حليف غير متوقع هو معهد ماساتشوسيتس للتكنولوجيا. وكان البعض في المعهد يعتقدون، ومن أبرزهم البروفسور هال إبلسون ومدير الشبكة جيف شيللر، أنه ينبغي السماح للمعهد بتزويد الأمريكيين ببرامج مسموح باستخدامها قانونياً ـ وأن يتم ذلك عبر الإنترنيت التي كانت أسرع وسيلة لتوزيع البرمجيات. وهكذا قام المعهد بتخزين أحدث النسخ من برنامج «منتهى السرِّيَّة»، في مخدم الإنترنيت، وسمح باستنساخها لمن يشاء ـ بعد شهادتهم بأنَّهم أمريكيون فعلاً.

إن الحكومة الأمريكية، لم تكن تفكر بنظام الوعود، وعهود الشرف حين وضعت قوانين التصدير. والحق أن الإجراءات التي أخذ بها المعهد لحماية الصادرات كانت من الهشاشة ما جعل عدداً من نسخ «منتهى السرِّيَّة» تلحظ خارج البلاد بعد يومين من عرض البرنامج. ومع ذلك فإن القيود المفروضة بما يخص الجنسية كانت كافية لتجعل معهد ماساتشوسيتس بمنأى عن المساءلة الرسمية، ناهيك عن التحقيق الجنائي. وليس مؤدى ذلك أن الحكومة كانت موافقة من الناحية الرسمية على هذا الترتيب. ففي جلسة مشهودة من جلسات مؤتمر عقد سنة 1995 وقعت مواجهة بين ممثل معهد ماساتشوسيتس جيف شيللر ومحامي وكالة الأَمن القومي رونالد لي (حل محل ستيوارت بيكر، عام 1994). فقد رفض لي أن يحدد ولو بشكل واه ما المسموح به وما هو الكفيل بأن يلقي بك في السجن، بالرغم من الطلبات المتكررة بأن يدلي ببيان يفصح فيه عما إذا كانت القيود التي وضعها معهد ماساتشوسيتس كافية. وفي تلك الأثناء كانت دار النشر الخاصة بالمعهد قد أصدرت كتاباً (هذه المُنتَجات الصناعية الشبيهة بالأشجار الميتة ما تزال حولنا) ولا يحتوي إِلاَّ مئة صفحة من الرموز بلغة البرمجة سي C بحيث يمكن لبرنامج منتهى السرِّيَّة، الذي وضع على نحو تستطيع معه الكاشفات وبرمجيات التعرف إِلىٰ الكلمات تحويل الكتاب المطبوع بسهولة إِلىٰ برنامج تشفير قوي ينتج على نطاق واسع. وبدا الأمر أقرب إِلىٰ الخيال أن يجيز القانون مثل هذا المخطط بينما هناك هيئة عليا من المحلفين ما زالوا ينظرون في إدانة فيل زيمرمان؛ غير أن هذه هي حالة الضعف التي كانت عليها سياسة تصدير برامج التشفير عام 1995.

ولقد واجه مجدد ثوري آخر في مجال الشّيفرة تطفلاً من عالم الواقع الشرس، وكان هذا يولف هيلسينجيوس المبرمج الفنلندي الذي كان يدير أول مدور للبريد وبالتأكيد أشد المراكز شعبية في العالم. وكان المشروع الذي يقوم عليه سنة 1995، يدعى بينيت، وهو مثل ساطع على فوضى التشفير، إذ كان

ينزع شارات التعريف عن آلاف الرسائل كل أسبوع، ثم يعيدها مغفلة لتسير في طريقها بسلام. وأصبح المشغل معروفاً في أوساط معينة وممقوتاً من المتنبئين باليوم الآحر في الحكومة الذين حذروا بأن خدمات كهذه، آتية لا ريب بنهاية المجتمع المتحضر. لكن المتاعب لم تأت من الحكومة بل من جماعة خاصة، الكنيسة العلمية.

كان العلميون، قد ضاقوا بما يصدر من النقد عن أعضاء قدامى حاقدين من جماعات جرت على عادة التداول والنقاش على شبكة الإنترنيت. وكان هؤلاء المبشرون يحصلون أحياناً على وثائق كنسية فيقومون بتوزيعها عبر الشبكة. وقد سعى بعض المسؤولين في الكنيسة العلمية إلىٰ مقاضاة هؤلاء الأشخاص لخرقهم حقوق الكنيسة الأدبية وأسرار المهنة. ولما كانت عناوين النقاد قد نزعت عن مراسالاتهم عبر نظام تدوير البريد، وتبين أنه غالباً ما كانت بينيت هي الجهة المخدمة، فلم يكن من اليسير اكتشاف الشخص المسؤول.

ثم تبين أن هناك فعلاً طريقة لاكتشاف المرسل. فقد كانت بينيت تسير بخطين ـ على العكس من الكثير من مدوري البريد، من زعران الشّيفرة ـ فأتيح بذلك للناس، الرد مباشرة، على الرسائل التي لا تحمل عنوان المرسل. وقد اقتضى هذا النُظام، وجود وسيلة لتعقب أصحاب الرسائل عبر نظام «يولف». فوجه محامو الكنيسة أولاً رسالة يحذرونه فيها بأن المصلحة التي يقوم عليها إنما تقوم بخرق حقوقهم الأدبية. فرد «يولف» بلغة لبقة مهذبة بأنه انتهج لشبكته سياسة عدم التدخل في ما يمر بالكومبيوتر. أفليس لديهم مدورون لبريدهم؟ ورد محامو الكنيسة بالتهديد بمقاضاته قانونياً، إذا ما استمر في انتهاك حقوقهم الأدبية. فاستبعد هيلسينجيوس، وهو في فنلندة، أن يقدم هؤلاء المحامون، الذين لا ملامح لهم، والمقيمون في كاليفورنيا، على اتخاذ مثل هذه الإجراءات. وفي تلك الأثناء سمع يولف هيلسينجيوس رنين الهاتف. وكان المتكلم، ممثل للكنيسة العلمية، بشحمه ولحمه. في فنلندة.

سأله ممثل الكنيسة إن كان يقبل دعوته إلىٰ العشاء؟

فقال يولف في دخيلته، أنه ليس في رفض وجبة طعام ما يرضي العقل. وكان الرجل يبدي في حديثه كل الود، وأخبره أنه رجل شرطة متقاعد، وما يبغيه منه أمران: التوقف عن توجيه الرسائل، وإعلامه بالطرف الذي يوجهها.

فرد هيلسينجيوس: «آسف! هذا أمر لا أقدر عليه». ولكن العلميين لم يكونوا يعتمدون، على حسن نية يولف هيلسينجيوس للوصول إلىٰ الاسم. فتقدموا عندئذ بشكوى إلىٰ شرطة لوس أنجليس، يدَّعون فيها أن ملكيتهم المسروقة يجري شحنها عبر الإنترنيت ووجَّهوا اصبع الاتهام إلىٰ هيلسينجيوس بأنه يتستر عمداً على اللصوص. وهذه في فنلندة جريمة خطيرة يكفي توجيهها ليحصل المدعي على أمر بالتفتيش وإلقاء الحجز على المادة المسروقة.

وبعد أسبوع من ذلك الاعتذار، ورد طلب الشرطي المتقاعد، تلقى هيلسينجيوس مكالمة أخرى من شرطة هيلسينكي. وأُعلم يومئذ بأن لديهم أمراً صادراً عن المحكمة يقضي بـ «مصادرة الكومبيوتر لتفتيشه». وهنا وجف قلب هيلسينجيوس وأدرك أن عليه إلاَّ الانصياع. (والمضحك المبكي في الأمر أن هذا البحث كان سيذهب أدراج الرياح لو أن هيلسينجيوس لجأ إلىٰ برنامج التشفير لديه ليرمز البيانات عنده ويوفر الحماية لزبائنه. ولكنه لم يلجأ لتشفير محتويات القرص لأسباب تتعلّق بقدرة [الكومبيوتر] ضخامة قاعدة البيانات، على حد قوله، حالت دون إجراء عملية التشفير).

ولما كان هيلسينجيوس يدرك أن العلميين، إنما يريدون منه أن يتخلّى عن عميل واحد، فقد نحا، إلىٰ عدم المجازفة بالآلاف الآخرين. وكان من حسن حظه أن استطاع الإفادة من العلاقة الطيبة القائمة بين الفنلنديين والشرطة، بأن عقد وإياهم اتفاقاً لا يقتضي منه تسليم كل محتويات قاعدة البيانات. وعمد عندئذ، إلىٰ نسخ عنوان البريد الإلكتروني الخاص بالطرف المعني على القرص

المرن، ووضعه على الطاولة بمتناول الشرطة. وقد علق على تلك الحادثة بقوله: «لم أكن سعيداً جداً بما حصل، إلاَّ أنها كانت تسوية».

غير أنَّه لم تكن تلك نهاية متاعب هيلسينجيوس، إذ كانت هناك مؤسَّسة أخرى في عالم الواقع، تهيئ لمداهمة استعراضه التشفيري الفوضوي: الإعلام. فقد نشرت إحدى الصحف السويدية هذه الحادثة في ذات اليوم الذي سلم فيه القرص للشرطة وادعت أن تقصي أثر معظم الصور الإباحية للأطفال على الإنترنيت قاد إِلىٰ مخدم في فنلندة. وغني عن القول أن هذه إشارة إِلىٰ بينيت. لكن «يولف» كان واثقاً من أن دائرته لم تقم بتوزيع مثل هذه المواد، لأنه كان قد أغلق «الثنائيات» (الصور الرقمية). ولقد شاعت القصة ولم يتجشم أحد عناء التحقق من صدق الخبر. فلما أخذ يلاحق مصدر المعلومات تبين له أن شبكة من الشبكات التي تقدم صوراً إباحية للأطفال كانت تزور الرأسية التي تتصدر الصور بحيث تبدو وكأن مصدرها موقعه بينما هي تبث من موقع في المملكة المتحدة. ومع ذلك فقد كان لتلك الأخبار المروجة أثرها المؤذي، وازداد الأثر سوءاً حين رددت صحيفة بريطانية هذا الادعاء، وأوردت هذه المرة اسم هيلسينجيوس بالذات باعتباره الوسيط الشرير، في برامج الأطفال الإباحية على الإنترنيت.

وفي غضون ذلك، استمرت دعوى كنيسة العلم؛ واستدعي هيلسينجيوس للإجابة أمام المحكمة، عن سبب عدم تسليم الأسماء الأخرى. وكان في غضون ذلك قد اتخذ إجراءاته لحماية أمن 700 ألف عنوان على قائمة البريد الإِلكتروني، وكانت هذه الأسماء ما تزال غير مشفَّرة حتى تلك اللحظة، إنما مخفية، إذ كان الرجل قد نقل الكومبيوتر من بيته إِلىٰ غرفة مستودع في مكان سري. ثم قام بتوكيل محامين لمتابعة قضيته، ويعلم الله أنه لم يكن يملك المال لإنفاقه في مثل هذا السبيل. وقد دافع عن موقفه أمام المحكمة الفنلندية أن من يفيد من خدماته، له كل الحق في التمتع بالخصوصية والسرِّيَّة. ولقد جزع حين

قضى القاضي بأنه لا ينبغي إيلاء البريد الإلكتروني الحماية ذاتها التي يتمتع بها البريد العادي. وكان من أثر تلك الواقعة، أن تراجع عالم الآلة خطوة إلى الوراء، على الأقل في فنلندة.

كان السيل قد بلغ الزبى، عند يولف هيلسينجيوس. فقال: كان القرار واضحاً: «لم يعد بوسعك أن تقوم بمخدم كالذي أقوم عليه في فنلندة. وهكذا كان إغلاق موقع شبكة بينيت يوم 30 آب/ أغسطس 1996. وكان الدرس المستفاد الذي لا مهرب منه هو أن التكنولوجيا وإن وفرت حرية التشفير فلا بد للناس الواقعيين من أن يعيشوا في عالم الواقع ـ حيث تتمتع الحكومات والمشرعون بالوسائل لملاحقتهم. إن لعالم الواقع، القدرة على تعقيد الأمور أشد تعقيد.

لقد كان بوسع ديفيد تشوم أن يعرض عليك هذا الدرس، أيضاً.

كان مخترع النقود الرقمية المجهولة المصدر ـ وصاحب أهم البراءات في مجال النقود الإلكترونية ـ يواجه وقتاً عصيباً وهو يجهد لتظل شركته ديجيكاش عائمة. ومع أنه توفر له جمع رائع من المبرمجين والكريبتوجرافيين في مقر شركته بأمستردام فقد كان ثمة ضيق متزايد أخذ يشيع بين أعضاء فريق العمل. كذلك كان تشوم قد قصر عن إكمال التحالفات الهامّة التي هو بحاجة إليها لتعميم أفكاره. ثم ازدادت المؤامرات داخل جماعته الصغيرة حدة حين زعم أحد طلابه القدامى ويدعى ستيفان براندس أنه ابتكر طريقة بديلة لطريقته في إنتاج نقود دون تحديد مصدرها وبدأ باستقصاء طرق لبيع هذه الأفكار. وقد أصر تشوم على أن عمل براندس يعتمد على بحوثه وطرائقه. (نال براندس على براءات اختراع نافذة). وكانت ديجيكاش، ما تزال تبحث عن الصفقة الكبرى.

كانت ديجيكاش، قد بدأت برنامجاً تجريبياً رائداً على شبكة الإنترنيت، يدعى النقود الإلكترونية E-Cash واستخدمت في ذلك ما يشبه النقود، نقود رقمية كلعبة المونوبولي. أما في الحقيقة، فكانت هذه تجربة لدراسة إمكانية

استخدام، نقود رقمية على الشبكة، شكل من النقود تحل ذات يوم، محل العملة الورقية والمعدنية. أما الآن فبوسع المستخدم أن ينال 100 «دولار آلي» بمجرد أن يستدعيها من الآلة. وكان ذلك كله يجري دونما معرف. كذلك كان يمكن إرسال هذه الأموال الرقمية بالبريد الإلكتروني إلىٰ الأصدقاء أو «شراء» ما يلزم من أي تاجر يقبل الدولارات الرقمية على سبيل التجربة. ومع أن دائرة المعارف ،لبريطانية قبلت بهذا الأسلوب في تسديد ثمن مطبوعاتها، فإن قلة من التجار قد قبلوا بالنقود الإلكترونية، وهؤلاء يدورون في مجال محدود جداً وفي نطاق عمليات محددة يعرض نسخاً مسروقة لمجموعة كوميدية لتحصل على أرباح الدولارات الآلية.

ولما أذاع تشوم نبأ عقد الصفقة، كان الطرف المالي مؤسَّسة في منطقة وسط غرب الولايات المتّحدة، ذات اسم مألوف عند طلاب الأدب أكثر منه لدى الممولين الدوليين: مارك توين بنك. وقد تم الاتفاق على تقديم نسخة من النقود الإلكترونية. حيث يمكن تحويل الوحدات النقدية الإلكترونية إلىٰ عملة حقيقية مكفولة من مارك توين. فإذا نجحت التجربة فقد تهرع المؤسَّسات المالية الأضخم إلىٰ تبني هذا الأسلوب. وهنا ربما وجد نقاد تشوم، ما يحملهم على الصمت، وكان أحد هؤلاء النقَّاد قد وصف أفكار تشوم بالخيالية والطوباوية كالتقاء بحيرة والدن [التي خلّدها المفكر الأمريكي ثورو في كتابه الموسوم باسم البحيرة، والدين. هـ. م] والإنترنيت.

ولم يكن تشوم وحده الذي يعاني المصاعب في إرساء النقد المشفّر ليكون معياراً تتعامل به الإنترنيت. إذ أن الصفقات التجارية لم تكن تقلع بالسرعة الكافية، ومعايير الشبكة كانت ما تزال، بعد، في طور التبلور، مما جعل استخدام أي نوع من النقد المشفَّر صعباً. وكان منافسو تشوم لا يعيقهم الالتزام الأخلاقي بضرورة إخفاء منشأ النقود الرقمية. فقد كانوا يرون على العموم أن الناس لا يهتمون بطلب مثل هذا الالتزام. ولكن تلك الشركات كانت

قد قصرت، عن تحقيق ما يتوقع منها، وكان من بين تلك الشركات شركة سايبر كاش وشركة مونديكس الحديثتان والمدعومتان بالمال، اللتان سمحتا للزبائن تنزيل النقود على بطاقات ذكية بحجم بطاقات الائتمان (فكر بآلة حساب مصرفية على كومبيوترك الشخصي). ولكن أين هذه من خيبات الأمل التي أصابت تشوم. لقد كان تشوم صاحب براءات النقود الرقمية المغفلة، ولما أعلنت ديجيكاش إفلاسها في النهاية، في عام 1998، كان تشوم ذاته الذي خسر تلك البراءات.

وبالرغم من المشكلات، والمضايقات التي خبرها أصحاب الثورة، في عالم التشفير في منتصف التسعينات فإن رسالتهم الكبرى كانت تمضي قدماً إِلىٰ الأمام. وبصرف النظر عن المناوشات والنكسات التي اعترضتهم فإن الحكومة هي التي كانت تفر أمام زحف هؤلاء الثوريين. فبعد تراجع آل جور الأول عن تعهده بتعديل خطة المقراض في كتاب إِلىٰ عضو الكونغرس كانتويل، عرضت الحكومة التوصل إِلىٰ تسوية مع أرباب الصناعة، ثم عقدت عدة اجتماعات في مقر المؤسَّسة القومية للمعايير والتكنولوجيا بماريلاند للتوصل إِلىٰ اتفاق. وكانت الآمال عظيمة بالتوصل إِلىٰ خطة ما تسمح بتحرير قواعد التصدير وترك موضوع وديعة المفتاح ليكون موضوع خيار حقاً. ولقد بدا بعض ما صدر عن الحكومة منطقياً تماماً. ولكن لما أزاح المسؤولون في الإِدارة الستر عن الأَنظمة النهائية تبين أن الشيطان يكمن في التفاصيل. وخلاصة القول أن القيود المفروضة على الصادرات سوف تستمر كما كانت دائماً، أما القوانين الخاصة بالمقراض فسوف يخفف منها جزئياً (كأن يكون للمستخدمين اختيار الوكالات لإيداع مفاتيحهم). ولقد فازت الخطة باسمها المستعار المقراض 2 بجدارة.

ولقد تلا المقراض 2 بالضرورة المقراض 3، عام 1996. وكان لهذه الخطة غرض جديد، وتقوم على التلويح للشركات المتعاونة بجزرة تنالها إذا وعدت بأن تقوم بوضع الوديعة في مُنتَجاتها مستقبلاً، ويسمح لها بتصدير شيفرة بقوة معيار تشفير البيانات، بدون إيداع فوراً. والأمر المريح الواضح هو إعفاء

شيفرة قوية إلىٰ حد ما من قيود التصدير لتأخذ الصناعة مجالها. ولكن الحكومة عمدت بدلاً من ذلك، إلىٰ طرح بدائل للسياسة المتبعة ذاتها، هي غير السياسة المطلوبة.

وكان ثمة مشكلة لم تنقطع، تلح على الحكومة، هي نظرة البلدان الأجنبية بعين الريبة، إلىٰ تصميم أمريكي يحتوي على مودع للمفاتيح. وهنا أرسل «سفير للشيفرة» إلىٰ الخارج لإقناع المجتمع الدولي بأن حلاً شاملاً كهذا الذي يحمله معه سيأتي بالفائدة للجميع. ولكن لما كان الحل لا يقدم في التطبيق مساواة بين كافة الدول في الوصول إلىٰ المفاتيح بات من المحتم أن تنتهي مهمة السفير إلىٰ الفشل. وقد رأى بعض أعضاء الحكومة في هذا المثلب الضربة القاتلة للسياسة كلها.

وفي تلك الأثناء أخذ الكونغرس بدراسة حل تشريعي للمشكلة، مدفوعاً بالشكاوي من الخسائر، التي تنزل بالصناعة الأمريكية، أمام الشركات الأجنبية التي تبيع برنامج الشيفرة. ففي عام 1996 قدم السيناتور ونراد بيرنز، عن ولاية مونتانا، مشروع قانون «الأمن والحرية من خلال التشفير» ينص على رفع القيود عن برامج، تقدم شيفرة من مستوى «مقبول عموماً». (يفترض بأن هذه الفقرة تشمل معيار تشفير البيانات وخوارزمية رسا التي تستخدم في الولايات المتّحدة. كذلك تناولت مسودة القانون المخاوف من أن تعمد الحكومة إلىٰ اعتبار تكنولوجيا المقراض أسلوب التشفير الوحيد المعتمد: نص مشروع القانون على منع نظام وديعة المفتاح. ولقد سر بيرنز للسمعة الجديدة التي اكتسبها باعتباره فارساً مدافعاً عن حرية التكنولوجيا الحديثة، وهو ابن الغرب الذي يرتاح لركوب ظهر الحصان أكثر من الجلوس أمام شاشة الكومبيوتر. غير أن مشروع القانون ذاته بقي حبيس ملفات اللجنة بينما ظل المشرّعون تحت تأثير جلسات المذاكرة المعدّة أحسن إعداد من رجال وكالة الأَمن القومي وهم يحذرون من تهديد الأَمن القومي. وقد عبر عن هذا الوضع، السيناتور باتريك ليهي، وكان

من أوائل المؤيدين للقانون المقترح، بشكواه، من أنَّه في الوقت الذي «يتفهم فيه بعض [المشرعين] هنا الموضوع تماماً، إلاَّ أن هناك آخرين يخوضون في الأمر وكأننا [في الأوضاع التي كانت سائدة قبل عشر سنوات، عن صناعة [تتطور بسرعة، حيث] تعتبر عشرة أيام كالأبدية».

لو كان هدف الحكومة مجرد المماطلة، كل يوم يمضي، وجدار السد قائم هو بمثابة نصر لنا، لحق اعتبار النهج الذي سارت عليه نجاحاً. ولكن هذه السياسة كانت تنطوي على مخاطر، كما برهنت الهجمات التي شنّها زعران الشّيفرة على البرامج المخصّصة للتصدير، وأظهر اعتراض المكالمات عبر الهاتف الخليوي، بما في ذلك التي تجريها الزعامة الجمهورية في الكونغرس ومجلس الشيوخ، بأجلى صورة. فالبلاد تفتقر لنظام أمن إلكتروني قوي، وهو ضعف ازداد خطورة مع ازدياد انتشار الإنترنيت بصورة أعمق، وتداخل الشبكة في نسيج الحياة الأمريكية.

كان هذا على الأقل أحد الاستنتاجات الرئيسة التي خلصت إليها دراسة أعدها مجلس البحوث القومي. وكانت تلك المنظمة، وهي ذراع البحث في الكونغرس، قد قامت بفحص شامل لسياسة الولايات المتّحدة والمتصلة بالشّيفرة والتشفير، مستعينة بجهاز من الخبراء من كافة الأطراف المعنية بالموضوع، وضمت وزراء سابقين ومسؤولين من وكالة الأَمن القومي والنقاد من الفعاليات الاقتصادية والجامعات، مثل راي أوزي ومارتي هيلمان. وجاء تقرير اللجنة، وكان بعنوان «دور الكريبتوجرافيا في تأمين مجتمع المعلومات»، شديد الانتقاد، على نحو مفاجئ، لسياسة الحكومة ونصح بالدأب على حرية ممارسة التشفير في الداخل، وتخفيف القيود على الصادرات وقبل كل شيء وضع «آلية لإشاعة الأَمن المعلوماتي في القطاع الخاص». وبعبارة أخرى، مزيداً من التشفير.

ولعل أَكثر الملاحظات أهمية، التي وردت في الدراسة، كانت نتيجة

لجلسات المذاكرة السرِّيَّة، التي حضرها أعضاؤها (حرم ثلاثة من أصل ستة عشر عضواً، من الموافقة الأمنية فلم يحضروا الجلسات). ومع أن أولئك الأعضاء امتنعوا عن كشف ما سمعوه في جلسات المذاكرة فقد كان بوسعهم تقدير أهمية تلك المعلومات السرِّيَّة في تحديد السياسة على المستوى القومي وهذا ما ورد في تقريرهم. الجواب: لم تكن بالأهمية العظيمة. فذكر التقرير أنَّه ليس لتلك «التفاصيل السرِّيَّة. . . صلة ذات شأن بالقضايا الأوسع من الأسباب التي تجعل السياسة تتخذ هذا الشكل وهذا الحال اللذين هي عليهما اليوم ولا بالصورة العامّة التي ستكون عليها التكنولوجيا ولا المنحى الذي يحكم تطور السياسة مستقبلاً». وحسبنا من هذا ما بلغنا من تفصيل القول: «لو كنتم تعلمون ما نعلم».

ولقد أصاب بعض القوم في الإِدارة حرج من هذه النتيجة. (بل قد ساد أوساط مجلس الأَمن القومي، شيء من الضيق، لأنه يمكن اختصار عنوان الدراسة بالإِنكليزية Cryptography's Role in Securing Information Society، بإعادة تشكيله من الحروف الأولى CRISIS، أي أزمة). وكانوا قد سلموا بأن جلسات المذاكرة السرِّيَّة كانت دقيقة شاملة، ولكنَّهم كانوا على قناعة من أن استيعاب المرء الموضوع على الوجه الصحيح عليه أن يحيا في عالم المخابرات ويتنفس هواءها. حقاً أن مارتي هيلمان أَو راي أوزي كان يدرك نظرياً أن مراقبة خط أحد المحتالين أَو اعتراض مكالمة إرهابي بالهاتف الخليوي أمر هام. ولكن الرئيس ونائب الرئيس يتلقيان كل صباح مجلدات ضخمة حسنة الشكل ترصد مختلف نقاط الضغط الحساسة في العالم، كل شيء من شيفرة التقارير الدبلوماسية إِلىٰ رصد مكالمات رجال المافيا الروسية عبر الهاتف في سيارته. وجماعة كلينْتون كانوا يعلمون جيداً أن التشفير إن شاع وعمّ فسوف يضيع منهم جزء عظيم من هذه المجلدات.

ولكن هذه النقطة الدقيقة لم تبلغ الجمهور الواسع، بل وفاتت العديد من

أعضاء الكونجرس، الذين كلفوا اللجنة بإجراء هذه الدراسة. وبدا تقرير مجلس البحوث القومي بدلاً من ذلك أشبه بدعوة إلىٰ السلاح، للإطاحة بالقيود السخيفة، المفروضة على الشّيفرة والبدء بتدعيم أنظمتنا الخاصة. وبعد فالجني كما قال التقرير قد خرج من القمقم. وبهدوء أخذ بعض أقوى المدافعين عن إخضاع الشيفرة لسيطرة الحكومة يقرّون بهذا الرأي، أيضاً.

ولقد فُتحت بعدئذ جبهة أخرى في حرب الشّيفرة. فلأول مرة أخذت أَنظمة التصدير، تواجه تحدياً جاداً في القضاء. وكان مدير وكالة الأَمن القومي بوبي رابي إنمان قد اطمأن إلىٰ نجاحه برد رأي محام بوزارة العدل سنة 1978 بأن أَنظمة التصدير تشكّل خرقاً للتعديل الأول للدستور [الذي يكفل للمواطنين كل الحرية دون عائق أَو تدخل. هـ. م]. غير أن هذا الموضوع ظل بمنأى عن النقاش، ولم يسبق أن تعرض له قاض من قبل. وكان العديد من الخبراء القانونيين قد رأوا أن الموضوع لو طُرح أمام المحكمة فإن القرار سيكون لصالح جماعة الشّيفرة. والحق أنه حين نظرت المحكمة قبل حين في دعوى أقامها أحد زعران الشّيفرة، فيل كارن، ضد قرار بمنع تصدير القرص المرن الذي يحتوي كتاب «الكريبتوجرافيا التطبيقية» قد أثار جدلاً مستعراً. فقد جاء قرار القاضي مبالغاً بالتشدّد. فقد رفض القاضي الفيدرالي المساواة بين المعلومات المتضمنة في كتاب مطبوع والمعلومات ذاتها بصيغة رقمية، وردّ الدعوى، ثم أدلى برأي مفحم على الطلب الذي تقدم به كارن، هو بالضرورة اتهام له بشنّ هجوم غير أخلاقي على الأَمن القومي. ولكن ذلك كان عرضاً ثانوياً لقضية أهم: قضية دانييل بيرنستين.

كان بيرنستين، طالباً يعد لنيل شهادة الدكتوراه من جامعة بيركلي، وبدأ اهتمامه بالشّيفرة والأمن سنة 1987 حين تمكّن أحدهم من التسلّل إلىٰ كومبيوتره ومعرفة حساباته، فرغب منذ ذلك اليوم بدراسة خوارزميات الشّيفرة في إطار دراسته الجامعية وليس ثمة دلالة على تغير الأزمان أكثر من أن مناهج الدراسة

التي تركز على دراسة الكريبتوجرافيا، أصبحت اليوم أمراً شائعاً. وجدير بالتنويه أن الأَنظمة الجامعية تحظر، من الناحية الفنية، على أي شخص أن يضع شيفرة مبتكرة في مكان يمكن أن يقع عليه أجنبي. وهذا بالضبط ما كان بيرنستين يريده.

كان مشروع بيرنستين يستلهم، صدفة، برنامجاً وضعه رالف ميركل عام 1989 يوم كان يعمل في زيروكس بارك، هو عبارة عن دالة تجميع ويدعى سنيفرو. كانت الإضافة التي قدمها بيرنستين إِلىٰ برنامج سنيفرو في إطار دراساته العليا، سنة 1990، في جامعة نيويورك كشف افتقار الشيفرات المعدّة للتصدير للمنطق. وكان يعلم أن برامج التشفير تخضع لقيود معينة، بينما الألعاب التي تتضمن دالة تجميع مثل برنامج ميركل مباحة (وهي لا تقوم بتعمية المعلومات لمجرد التعمية وحدها). وهكذا وضع بيرنستين برنامجاً يحول برنامج سنيفرو إِلىٰ برنامج يؤدي وظائف التشفير وتفكيك الشّيفرة (انظر إِلىٰ سنيفرو باعتباره سلاحاً أوتوماتيكياً محظوراً تم شحنه وتمريره عبر الجمارك بدون زناد والبرنامج الجديد هو العدة لتركيب الجزء المفقود). وقد شرح ابتكاره في ما بعد بقوله: «إنه قادر على معالجة أي دالة تجميع برمجية ويجعل منه أداة تشفير جيدة». وكان أن أطلق على ما ابتكره وهو رزمة التشفير هذه اسم «خنخنة» Snuffle، ثم أرفقه ببحث يشرح العمل الذي قام به. ولكن الرجل كان قلقاً من أمر نشر برنامجه، خشية أن يثير بإبرازه هذه الناحية، ضيق الحكومة». وهكذا وضع البرنامج على الرف.

لكن بيرنستين أعاد النظر في الأمر، وهو في بيركلي، سنة 1992. فلم لا يقوم بنشر برنامجه؟ وما الضير في ذلك وهو ليس إِلاّ تمريناً أكاديمياً، لا سلعة تجارية تعرض للبيع. ولما كان التشفير الفعلي يعتمد على خوارزمية مطبوعة ـ وهو لم يقدم خوارزمية تشفير أصلية من ابتكاره ـ فإنه لا يطرح تهديداً للجمهورية، فلمَ يكون نشره مشكلة؟ وكان المكان الواضح لنشره مجموعة

مناقشة الشّيفرة Sci. crypt discussion group. ولكنه قرَّر أن يتخذ قبل ذلك: إجراء احترازياً أخيراً، ليتأكد من أنه لا ينتهك بعمله القوانين. وكان أن سأل أحد الأشخاص في الحكومة، إذ كان ذلك مسموحاً به؟

ولقد كان من شأن هذه الخطوة الصغيرة أن تبعد البرنامج عن الإنترنيت طوال ما تبقى من القرن العشرين.

كانت المشكلة الأولى التي واجهت بيرنستين هي تحديد الدائرة الحكومية المختصة، بمعالجة طلبه. وبعد سلسلة طويلة من الأسئلة انتهى أخيراً إِلىٰ ما يطلق عليه اسم مكتب رقابة تجارة المواد العسكرية. وقام عندئذ بتوجيه كتاب إِلىٰ هذه الدائرة في حزيران/ يونيو 1992. وكان أن تلقى الرد الذي أثار غضبه والذي يحمل توقيع مدير ذلك المكتب الغامض، وليم بي روبنسون، ويؤكد أن توزيع البرنامج دون ترخيص يجعل بيرنستين عرضة للمساءلة القانونية.

قال بيرنستين في خلده، حسن، سوف أقوم بالإجراءات الشكلية للحصول على حق التصرّف بالسلع. ولكنه أمل أولاً بأن يقوم مكتب رقابة تجارة المواد العسكرية بتوضيح حقوقه وما هي السُّبل التي يمكنه اللجوء إليها في حال عدم موافقته على قرار من طرف الحكومة. وانتظر الرجل حتى آذار/ مارس 1993 حتى وجد من يتحدث إليه. وأخيراً استطاع حمل تشارلز راي، المساعد الخاص لوليم بي روبنسون، على مكالمته. (قام بيرنستين بتسجيل المكالمات، بإذن رسمي). فأخبره راي أنه، بصورة أساسية، لا وجود لأي حقوق له. فلو وضع البرنامج على الشبكة بدون ترخيص، ثم قام عدو للولايات المتّحدة بنسخه في قاعدة للإرهاب في أفغانستان أَو شقة في باريس فقد يكون مآل بيرنستين السجن ليكون بيته الثاني. ثم أخبر راي أن «ليس هناك استثناءات في هذا الموضوع. فإذا كنت تملك ما يعتبر معلومات فنية وفق لوائح الذخيرة. . . فلن يكون لك ملجأ سواء كنت من رجال الصحافة أم الجامعة. . .

فإنك تظل عرضة للمحاكمة». وسأله بيرنستين: «ولكن ماذا عن التعديل الأول».

وكان تفسير تشارلز راي، لدستور الولايات المتّحدة، أن «تلك الحرية تحمل معها مسؤولية الانصياع للقوانين والأَنظمة السارية».

وبعد شهر أمكن لبيرنستين الوصول إِلىٰ رئيس راي، وليم روبنسون الذي أكّد له ضرورة الحصول على إجازة رسمية لتصدير السلع CJ قبل القيام بتوزيع برنامجه. وقام بإجراء عدة لقاءات مع المسؤولين وكانت المحادثات معهم أكثر تثبيطاً للعزائم. وعلم أن ليس إيداع البرنامج وتوزيعه على الشبكة محظوراً وحسب، بل إن بيرنستين يصبح عرضة للمحاكمة. إذا ما وضع نسخة من بحثه في مكتبة عامة أيضاً. وبطبيعة الحال أصبحت وكالة الأَمن القومي طرفاً في الموضوع، شأنها دائماً، حين يتعلق الأمر بقضايا تتعلّق بتصدير أَنظمة شيفرة جديدة. وفي النهاية تمكن بيرنستين من إجراء بعض المحادثات مع ممثلين لوكالة الأَمن القومي، بعدما بلغه أن هناك وراء السياج الثلاثي من يعتبر برنامج «الخنخنة» Sunffle أداة «استراتيجية». وقد استنتج من ذلك أن البرنامج لا يسهل تفكيكه. ثم «أبدوا مساعدتهم لإعادة كتابة البرنامج حتى تنتزع منه مقوماته الاستراتيجية». ولكن بيرنستين اعتبر عملاً كهذا ضاراً.

وإذن عليه أن يخوض هذا السجال. ففي أيلول/ سبتمبر 1992 قدم خمسة طلبات، منفصلة للسماح بالتصدير. ثم قام بتجزئة المشكلة إِلىٰ خمس نسخ مختلفة ـ وهي تتراوح بين وصف للنظام بالإنكليزية، وعرض لصيغ رياضية ـ «لمعرفة ما هو مسموح به وما هو ممنوع». وهل يمكن للحكومة اعتبار كل جزء «مادة عسكرية»؟ كان بيرنستين ما يزال يعتقد أن الضباب سينقشع عن عيني أحد البيروقراطيين فيدرك أخيراً أن برنامج «خنخنة» مجرد بحث أكاديمي قام به طالب يحضر لدراساته العليا، وليس سلاحاً. ولكن الحكومة ردّت على تساؤلاته، في تشرين أول/ أكتوبر 1993، بقولها أجل، إن كل صيغة

رياضية أتى بها هي سلاح «يخضع للقوانين والأَنظمة التي تأخذ بها وزارة الخارجية».

الحق أن بيرنستين لم يدخل العمليَّة دخول مثير للشغب، ولكنه وجد نفسه الآن ثائراً مُستفَزاً. وراح يتابع القضية بصبر وتأنٍّ وعقل منهَّج على نحو كان له الأثر المدمر لدفاع الحكومة الأمريكية لاحقاً عن أَنظمة التصدير كما طبقت على برنامجه. فقدم استئنافاً عن استمارة إجازة التصدير CJ الأولى. فلما مضت الشهور ولم يبلغه ردّ الحكومة رأى أن ينشد المساعدة.

كان نصيره في هذه القضية شخص يدعى جون جيلمور، وهو رجل اعتاد خوض المعارك في المحاكم ضد الحكومة. وكان هذا المشاغب المخضرم بين زعران الشّيفرة قد جمع لديه خزانة كاملة من الوثائق والعرائض التي تتصل بحرية تدفق المعلومات، وكانت في الأصل قيد السرِّيَّة ثم أفرج عنها بأوامر قضائية. نصح جيلمور بيرنستين بالاستعانة بمحامية تدعى سيندي كون وقد قبلت هذه المحامية بالمرافعة في القضية للصالح العام. (قامت مؤسَّسة الآفاق الإِلكترونية EFF بتغطية تكاليف الدعوى وتنسيق العمل مع محام مساعد). وفي عام 1995 تقدم بيرنستين ومؤسَّسة الآفاق الإِلكترونية بشكوى ضد وزارة الخارجية مدعين بأن قوانين التصدير مخالفة للدستور. وكان في مركز القضية الادعاء بأن نص البرنامج الأساسي في جهاز الكومبيوتر عند بيرنستين هو شكل من النطق والحديث والحكومة بمنعها نشره، إنما تنكر على بيرنستين حق التعبير.

وها قد أصبح الرأي الذي صدر في 1978، والقائل أن الأَنظمة قد تتجاوز التعديل الأول أخيراً أمام الامتحان. ولكن قلة من الناس وحسب كانوا يعتقدون بأن القاضي ربما عارض رأي الإدعاء الذي لا بد وأن تطلع به الحكومة، والقول بأن لقوانين التصدير أهمية حاسمة للأمن القومي، ولا بد وأن يؤدي القضاء عليها إِلىٰ ظهور الفرسان الأربعة في سفر الرؤيا في صورتهم المعاصرة:

تجار المخدرات المختطفون وتجار صور الأطفال الفاضحة، والأفلام الفضائحية والإرهابيون.

ولقد عرضت القضية، أمام القاضية مارلين باتيل في محكمة منطقة شمال كاليفورنيا. . ولم تكن تصرفاتها الأولى تدعو للارتياح في نظر الادعاء، إذ أمرت بختم الأدلة، نظراً لأن قوانين التصدير تحظر توزيعها. ولكن القاضية باتيل أظهرت مع متابعة الدعوى تعاطفاً قوياً مع دعاوى بيرنستين. ولعل الحكومة لاحظت هذا التعاطف فلجأت إلىٰ عدة تكتيكات لتنتزع الدعوى من محكمتها. وقد ناقضت الحكومة نفسها في استمارتين من أصل الاستمارات الخمس التي قدمت، فاعترفت بأن تلك الآراء الرياضية كانت مجرد «بيانات فنية». ثم عمدت إلىٰ الطعن بصلاحية محكمة القاضية باتيل النظر في قضايا تتصل بقوانين التصدير. وطلبت عندئذ برد الدعوى على هذا الأساس. ولكن القاضية باتيل قرَّرت يوم 27 نيسان/ أبريل 1996: استمرار النظر في القضية. وكان المسوغ الذي اعتمدته كافياً لإثارة القشعريرة في بدن واضع الأنظمة: فقد رأت القاضية مارلين باتيل أن بعض القيود المفروضة على تصدير برامج التشفير، على الأقل، مخالفة للدستور. ثم قبلت فوق هذا، بادعاء فريق بيرنستين أن نص البرنامج الأصلي يمكن اعتباره شكلاً من الحديث. وكان هذا يعني سريان القواعد الأشد صرامة التي نصّ عليها التعديل الأول للدستور. والمتعلق بتقييد الحرية ويتصل بطلب الإذن المسبق إنما ينطبق على هذا البرنامج. وبالنسبة إلىٰ موضوع الدعوى التي تنظر فيها باتيل فالأمر لا يتعلّق بالمحافظة على سلاح داخل الحدود؛ بل إن الموضوع هو منع غير شرعي لحرية التعبير وهذا مخالف للدستور وكان أن أكّدت باتيل في ذلك الصيف قرارها الأولي.

استأنفت الحكومة قرار المحكمة أمام محكمة الدائرة التاسعة الأعلى. وكان بيرنستين قد نال في تلك الأثناء شهادة الدكتوراه، وانتقل إلىٰ شيكاجو

للتدريس في جامعتها. وهناك، رغب في تدريس منهاج، يتضمن الكريبتوجرافيا، ولكنه بسبب من استمرار الدعوى كان بحاجة لموافقة الحكومة على تدريس هذه المادة. فتطلب الأمر قراراً قضائياً آخر قبل أن يسمح له أخيراً بتوزيع المواد المتعلقة بعمله ـ على طلابه حصراً. وهكذا جرى تدريس ذلك المنهاج دون أن يترتب على ذلك ضرر ملحوظ للأمة.

ومع ذلك فقد استمرت القضية، أمام المحكمة بين أخذ وردّ. ثم تقرَّر عقد جلسة للمناظرة الشفهية أمام مجلس مؤلف من ثلاثة قضاة، في شهر كانون الأول/ ديسمبر 1997. وشاءت الحكمة السائدة يومذاك، أن تلغي محكمة الاستئناف ما اعتُبر قراراً غير متبصّر من قاض يجلس على كرسي المحكمة، في نهاية المطاف، في سان فرانسيسكو التي يشيع فيها السخف. ولكن القضاة راحوا، في قاعة المحكمة المزدحمة بالحضور، يوجهون أسئلتهم بلهجة قاسية إلىٰ محامي الحكومة الذي غلبت عليه سلاطة اللسان والإزعاج. وبدا القضاة يومئذ أكثر إعجاباً بمحامية بيرنستين سيندي كون، وكانت امرأة ضئيلة الجسم في أوائل الثلاثينات من عمرها، تقدم حججها بقوة بالرغم مما كان يعتور صوتها من تردد بين الحين والآخر. وكان ثمة نقطة مفاجئة أوردتها المحامية، وهي أن الحكومة حينما قامت بمنع عملية النشر على شبكة الإنترنيت لم تنتبه إلىٰ قرار اتخذته المحكمة العليا مؤخراً ويعلق قانوناً يعرف بقانون آداب الاتِّصالات Communication Decency Act، إذ رأت المحكمة أن الشبكة منارة للديمقراطية ولها الحق بأعلى مستوى من الحماية التي نص عليها التعديل الأول. كذلك ألحّت كون على القضاة النظر إلىٰ المضامين التي ينطوي عليها، قطع أسباب الحياة عن التشفير؛ وتساءلت إن كان يليق بالحكومة أن تمنع الأدوات التي قد يحتاجها مواطنيها لضمان خصوصياتهم.

ظل القضاة الثلاثة ينظرون في القضية مدة تزيد عن عام، ولم يصدروا قرارهم حتى أيار/ مايو 1999. وكان ذلك لدانييل بيرنستين قراراً يستحق الصبر.

فقد عبَّر القضاة، بأغلبية اثنين مقابل واحد، عن رأي واسع، لا يثبت قرار باتيل وحسب، وإنما زاد بالاحتفال بالكريبتوجرافيا باعتبارها من مقومات الديمقراطية، وعنصراً حيوياً في تكوينها فلا ينبغي أن يكون التشفير مجرد سر من أسرار الدولة، على ما جاء في القرار، وإنما حامياً لخصوصيات الناس أيضاً. وقد نم هذا القول عن أن القاضيين أدركا بطريقة من الطُّرق جوهر التشفير، دون أن يكونا قد تلقيا ثقافة علمية في هذا الموضوع. فكتبت القاضية بيتي فليتشر أن «محاولة الحكومة السيطرة على التشفير قد لا تقتصر آثارها على النيل من حقوق الكريبتوجرافيين التي كفلها التعديل الأول وحسب، بل ستنال من الحقوق الدستورية التي يتمتع بها كل منا، نحن الذين قد تصيبهم نعمة التشفير».

أقالت نعمة التشفير؟ لقد كانت القاضية فليتشر أحد زعران الشّيفرة متخفياً في زي قاض!

كان بيرنستين في شيكاجو يشرف على امتحان في مادة رياضيات التفاضل، في عصر ذلك اليوم الذي صدر فيه قرار المحكمة، ولم يعلم أنه أصاب الحكومة بضربة إلاَّ بعد ذلك الوقت حين نظر في رسائل البريد الإلكتروني.

استأنفت الحكومة، طبعاً، الحكم الذي أصدرته المحكمة ـ ولكن أَنظمة التصدير التي كانت تدافع عنها بدت أقرب إِلىٰ التداعي. لقد صمد السد في وجه التشفير طوال سنوات بشكل يدعو للإعجاب. ولكن السد أخذ الآن ينهار.

كانت هذه لعبة النهاية للحكومة.

والغريب أن وكالة الأَمن القومي، لم تعد تبدو العقبة الرئيسة في عملية التوصل إِلىٰ حل، وبوسع المرء أن يتبين عند السياج الثلاثي، قبولاً واستسلاماً بحقيقة التشفير الجديدة. بل إن كلينت بروكس ذاته لم يعد في الخطوط الأمامية، ولكن في النهاية قبلت المؤسَّسة التي قام على خدمتها بفكرته عن التغير. ولعل قادتها وجدوا أنَّه من الأفضل أن يوجهوا جهودهم للاستعداد لما

هو قادم، بدلاً من محاولة الوقوف في وجه التقدم. ولعل أساطين الشيفرة في وكالة الأَمن القومي رأوا بعد إمعان الفكر أن كابوس شيوع التشفير في كل مكان أمر يستطيعون التعامل معه إن توفر لهم المزيد من الأموال. وكما ألح روبرت موريس في كلمته أمام مؤتمر كريبتو 95، وتفكيك زعران الشّيفرة [لبعض البرامج] تشير إِلىٰ أن، هذه البرامج البرَّاقة، والتي «لا يمكن تفكيكها» التي ابتكرها القطاع الخاص هي في الحقيقة ليست بالعصية إِلىٰ هذا الحد، وكانت وكالة الأَمن القومي على اقتناع بقدرتها على الحصول على النص الواضح للرسالة المشفَّرة متى شاءت. وهناك شاهد على ذلك هو العمليَّة التي موّلتها وأشرفت عليها مؤسَّسة الآفاق الإِلكترونية: حيث قام فريق من المهندسين برئاسة جون جيلمور وبول كوتشر بصنع آلة تفيك معيار تشفير البيانات بكلفة 210 آلاف دولار (كان معيار تشفير البيانات ما يزال يعتبر ذخيرة حربية خيرة يحظر تصديرها إِلىٰ الخارج في الظروف العادية). وفي العرض الذي قُدم في مؤتمر كريبتو 1998، تمكّن الجهاز من إنتاج النص الواضح لرسالة مشفَّرة بمعيار تشفير البيانات في أقل من 24 ساعة. وغني عن البيان أنه إذا أمكن إنتاج هذه الآلات على نطاق واسع، فإن كلفة الحصول على مثل هذه المفاتيح تصبح زهيدة. وللمرء أن يفترض، بأن في أقبية وكالة الأَمن القومي الكثير من هذه الوحدات.

على كل حال، كان مكتب التحقيقات الفيدرالي، وخاصة مديره لويس فريه، هو الجهة التي ظلَّت تحثّ على الأخذ بالخط المتشدد إِلىٰ حد الاستمرار في الإصرار على أن يتمتع المكتب بحرية الوصول إِلىٰ النص الواضح ولو كلف الأمر تنظيم التشفير داخل حدود الولايات المتّحدة. واستطاع فريه في النهاية أن يحرر نسخة من مشروع قانون الهاتفية الرقمية، لإجبار أهل صناعة الاتِّصالات على ما يفترض لتصميم منتجاتهم على نحو يسمح بمراقبتها ودياً. (غير أن معارضي هذا التصور في الكونجرس أفشلوا مسعى دعاته بالامتناع عن تخصيص

مئات ملايين الدولارات المطلوبة لتنفيذه). ومع ذلك، فقد ظل فريه يخشى أن يؤدي التشفير إِلىٰ موت رصد الاتّصالات. ولقد دأب منذ عام 1994 على المطالبة علناً بأن يفتح الكونجرس عهداً جديداً من الحظر سمته منع التشفير الفعَّال دون مفتاح مودع، إذا لم يتمكن عملاؤه من الحصول على النص الصريح من عمليات الرصد. فقال: إن الهدف الذي نسعى إليه هو معرفة تلك الحوارات التي تجري عبر وسائل الاتّصال سواء تمت بواسطة مشابك التمساح أم بالواحد والصفر [رقمياً] إني أريد الحصول على هذه المعلومات، مهما تكن، ومهما يكن الطرف فيها». لكن فريه، كان قد فقد حظوته لدى إِدارة كلينتون فلم يأخذ المسؤولون فيها بملاحظاته، وضربوا عنها صفحاً.

ولا يقصد من هذا القول، أن الإِدارة قد تخلّت عن آمالها بالقضاء على موجة الشّيفرة. بل إن كل ما في الأمر هو أن رؤاها المعادية للتشفير، كانت تتضاءل وتزداد تضاؤلاً مع كل واقعة جديدة. وكان المشايعون في البيت الأَبيض يؤكدون أن هذه التبدلات أملتها روح آل جور واستعداده للتعاون مع المستثمرين في عالم التشفير وإيجاد التوازن المناسب بين الشّيفرة وراصديها. لكن جماعة كلينتون إنما كانوا يسيرون باتجاه واحد ليس له آخر إِلىٰ الوراء. وقد أقرّ بذلك مايك نيلسون بقوله: «كان المركب تحت القصف»؛ وليس من علامة تدل على أن السياسة تواجه ورطة كبرى أبلغ من أن الكلمات المستخدمة في وصفها تلقى أشد التنديد بحيث أنَّها تحتاج للتلطيف والتشذيب لتكون مستساغة، حتى أن كلمة وديعة بالإنكليزية Escrow غدت سنة 1979 كلمة نابية، بالرغم من أن آلاف الهواتف المزودة بالمقراض كانت قد بيعت في الأسواق في ذلك الحين، ومفاتيحها تجمع الغبار الرقمي في الأماكن المحددة للإيداع. وقد بلغنا الآن مرحلة أصبح الهدف المعلن، يسمى استعادة المفتاح. وإن تلك السياسة التي بدأت بضوابط المقراض الصارمة ـ خوارزميات سرِّيَّة في عتاد منيع، وخزائن وديعة، وتجهيزات للودائع تسيطر عليها الحكومة ـ قد جرى

تعديلها لتصبح مخططاً يعتمد على برمجيات، بحيث يستطيع المستخدمون اختيار تجهيزات الإيداع الخاصة بهم. وكانت هناك تسوية أخرى؛ فقد تم إشهار خوارزمية سكيبجاك (الوثاب) بعدما كانت في الماضي سراً محروساً بعناية. وقال أحد المسؤولين في الإدارة فيما بعد، في تفسيره لما حصل: «إننا لسنا أغبياء. لقد أصغينا إلىٰ السوق ومشينا». لكن السوق ـ والمقصود به الناس الحقيقيون الذين يسعون لشراء وبيع واستخدام برامج التشفير ـ لم يكن يريد شيئاً من برنامج الوديعة.

وفي غضون ذلك، كان الكونجرس يتلمس في نفسه الثقة، ليتابع مقتضيات السوق، بدلاً من أن يقع ضحية السيناريوهات الرهيبة التي تقدمها الإدارة منذرة بيوم القيامة الوشيك. ولعل العامل الأهم في هذا النزوع كان ظهور جهد ضاغط حسن التنظيم يمثل صناعة الكومبيوتر. فمنذ انقضاض النائبة ماريا كانتويل الانتحاري على قوانين التصدير ازدادت معرفة جمهور التكنولوجيا المعقَّدة، واكتسبوا الكثير من الدراية بقدرات كتيبة الأحذية البيضاء [الإدارة الأمريكية هـ. م] وما يمكن أن تلحقه بهم. فقد جعل المحاربون ضد الأنظمة، أمثال بروس هاينمان من اتحاد أصحاب البرمجيات من التشفير قضيتهم وجعلوا منها قضية حياة. وكانت التحالفات التي أقاموها مع جماعات الحقوق المدنية مثل مركز معلومات السرِّيَّة الإلكترونية، ومؤسَّسة الآفاق الإلكترونية، ومركز الديمقراطية والتكنولوجيا، توفر لهم الآن قاعدة شعبية من الناس العاديين. وكان أن التقت قوى الضغط مع المسؤولين ذوي الكلمة النافذة في الإدارة وأكثروا اللقاءات حتى كان يكمل أحدهم كلمة الآخر قبل أن تكتمل الجملة. وتمكنوا بالدهاء من معرفة المشرعين الذين يؤيدون مشاريع القوانين المتعلقة بالتشفير، ليس ليتجاوزوهم إلىٰ سواهم، وإنما لزيادة الضغط لإشاعة جو من الانفراج الشديد لصالح التشفير. وكان من أبرز من كسبتهم قوى الضغط النائب الجمهوري المحافظ عن ولاية فيرجينيا، روبرت جودلات، وديمقراطية من

دعاة الاقتصاد الجديد من وادي السيليكون، زوي لوفجرن. وكان جودلات بالأخص، متقداً شديد الحماس لهذا الموضوع، عبقرية ولدت حديثاً في الكتابة بالشّيفرة كأنما رسمت الإبرة خطوطها بدقة. قال هاينمان: «كان أول ما فعلنا هو أن ندعه يمضي بعض الوقت مع مسؤولي وكالة الأَمن القومي ليسمع وجهة نظر الطرف الآخر». وبعد أن اكتسب المناعة بفضل جلسات المذاكرة والاحتكاك المباشر والاطلاع على المعلومات السرِّيَّة، عرض له الوجه الآخر من الواقع، وهو التشفير أو الكتابة المعماة باتا مطروحين في الخارج، والصناعة تواجه خسارة بلايين الدولارات وإلخ. وما أن اعتاد عضو الكونجرس رؤية الغريب [عن وسط الحكومة هـ. م] حتى بات يظهر في أغلب الأحيان، مع كبار أهل صناعة الإنترنيت ومن المؤسف أنَّه صار هدفاً للنقد وسهامه.

ولقد أخذ جودلات ولوفجرن، يوضحان لزملائهما، بمساعدة جماعة حديثة العهد من أرباب الصناعة أطلقت على نفسها اسم «الأمريكيون من أجل سرِّيَّة الكومبيوتر» (كان هؤلاء «الأمريكيون» يتألّفون من ثلاث عشرة شركة منها الآر إس إيه، والآي بي إم، ونوفيل، والصن، ومايكروسوفت)، ما قد ينطوي عليه تأييد نظام تشفير قوي من فوائد سياسيَّة. وفي مجلس الشيوخ وقف فارس غير متوقع هو كونراد بيرنز عن ولاية مونتانا ليتصدَّى للحكومة، بمؤازرة المتبحّر في الخصوصية والسرِّيَّة باتريك ليهي والسيناتور ممثل مايكروسوفت باتي موراي، عن ولاية واشنطن.

وفي تلك الأثناء أخذ شكل مختلف كل الاختلاف عن المذاكرات المعهودة بالشيوع في قاعات الاستماع. فبدلاً من الأحاديث المستهلكة عن استمرار نجاحنا في تفكيك الشيفرة، أخذ الشهود يحذرون من وقوع كوارث محتملة نتيجة عبث الغرباء بأنظمتنا وهي قابلة للنيل منها، جزئياً، لأن أكثر دولة في العالم تقدماً قصرت عن اعتماد شيفرة قوية لحماية هذه الأَنظمة. وكان يبدو أن كل تخريب يصيب موقع الشبكة وكل سرقة لأَرقام بطاقة اعتماد على الشبكة

كان يدعم تلك المخاوف؛ وأخيراً أصبحت النتائج التي توصّل إليها المجلس القومي للبحوث تكتسب صدى. بل لقد نال موقع مكتب التحقيقات الفيدرالي على الشبكة نصيبه من الضرب! كذلك أصاب موقع مقام الكونجرس تشويش فجأة مع احتمال وقوع هجوم رقمي يماثل الهجوم الذي وقع على بيرل هاربر، حيث يتعاون المتسربون إِلىٰ الشبكة والإرهابيون وأمم معادية ويتمكنون من شل حركة مجتمعنا بإغلاق المراكز التي تعمل في بلادنا مثل شبكة الكهرباء أَو منظومات الأسلحة التي يحكمها الكومبيوتر. وإن لم يكن هناك رصاصة سحرية تعوض عن دفاعاتنا فالصحيح كذلك أن لدينا أداة قوية نحمي بها أنفسنا، هي شيفرة قوية، أي ما كانت الإِدارة تسعى إِلىٰ منعه!

في عام 1999، كان الكونجرس، الذي اكتسب الآن جرأة وجسارة، قد أخذ بالتجمع وحشد التأييد لمشروع القانون «الأمن والحرية بالتشفير» SAFE، الذي مضى على تقديمه ثلاث سنوات ويهدف إِلىٰ التخفيف من أَنظمة التصدير. والواقع أن الغالبية العظمى من أعضاء المجلس التشريعي ـ 258 عضواً ـ كانت قد وقَّعت على مسودة القانون بوصفهم مؤيدين له. ولم تكن الأخبار الآتية من مجلس الشيوخ أحسن حالاً من منظور الإِدارة. وكان القائد الذي تولى النضال والكفاح من أجل الوصول إِلىٰ تخفيف الرقابة على الصادرات، هو جورج ماك كين، وكان أسيراً في فييتنام، ولا تشوب مصداقيته في هذه الأمور شائبة. أما مشروع القانون الذي قدمه ماك كين والسيناتور بوب كيري في حزيران/ يونيو 1997 فقد اتسم بحظر قيام «سلطات توثيقية» من أية حكومة في المستقبل، (والسلطات التوثيقية هذه هي مؤسَّسات تتولَّى توزيع المفاتيح العامة والتعريف بها، وهي مكون ضروري في البنية التحتية للتشفير الكامل) بتقديم الخدمات لأولئك الذين يمتنعون عن إيداع مفاتيحهم. وفي ذلك ما يتيح للمواطنين الخيار بين استخدام الخطط من نوعية المقراض أَو حرمانهم من المشاركة في الجماعة الإِلكترونية. ولكن ماك كين عاد في عام 1999 فأمعن

النظر في الموضوع (وربما في أثرها على ترشيحه المنتظر لمنصب الرئاسة). وفي انقلاب مذهل، تحول ماك كين إِلىٰ السيد كريبتو، وبات يجاهر بتأييد مشروع الأمن والحرية بالتشفير.

فهل كان الوقت قد حان، لترمي الحكومة باستمارات التصدير في الهواء وتصيح «ليحيا النص المشفر»؟ هذا ما يبدو. فمع أن الحكومة لم تكن لتؤمن بأن الكونجرس سوف يقر مشروعاً يطلب تحرير الصادرات كان النِّظام أشد تعقيداً من أن يمد المرء يده إليه، والمجازفة بتعريض الأَمن القومي بالغة الحرج، وعلى كل حال هناك دائماً الفيتو الرئاسي الموعود ويمكن اللجوء إليه كان البيت الأَبيض في ضيق وقلق من أن تبقي الأصوات في اللجان الفرعية الموضوع حياً. وإذا شئنا الدقة قلنا أن جماعة كلينتون كانت قد أخذت تقلب التداعيات المحتملة لكارثة قومية تنجم عن فقدان التشفير وهو أمر تقع اللائمة فيه عليهم. فعلاً إن السماح بتصدير برامج تشفيرية أمر ينطوي على خطورة، كانوا يقولون، فقد يموت أناس لهذا السبب. . . ولكن الناس من جهة أخرى قد يموتون إذا ما هاجم شخص بنية رقمية تحتية! لكن المسألة كما عرضها أحد صانعي السياسة في البيت الأَبيض هي كيف يموت هؤلاء: هل تريد لهم أن يهبط عليهم الموت من السماء بصاروخ من الأرض إِلىٰ الجو، أم بنسف أبواب سد جراند كولي؟» فإذا اختصرت المسألة بستة من طرف مقابل اثني عشر على الطرف الآخر، فأي معنى يكون عندئذ، لمعركة صعبة مريرة لا خير يُرجى من ورائها؟

في أيلول/ سبتمبر 1999، أعلن آل جور، وكان يتهيأ هو ذاته للترشيح إِلىٰ البيت الأَبيض، أن هناك عدداً من القرارات سوف تصدر في كانون الأول/ ديسمبر وتسمح بتصدير منتجات تشفيرية موجهة للمستهلك مهما يكن طول مفاتيحها. وكان هذا تحولاً كبيراً إِلىٰ حد لم يستطع معه عضو الكونجرس كورت ويلدون، عن ولاية بنسلفيانيا، وكان قد ساعد الحكومة، في رد مشروع قانون «الأمن والحرية عن طريق التشفير»، أن يتمالك نفسه، فصاح:

«كيف بوسعكم أن تعملوا بهذه السياسة؟ لقد دأبتم على القول لنا، طوال سنوات، بأن من شأن طرح شيفرة قوية، أن تعرض الأمن للخطر، وتمنح المجرمين قوة وسلطة. وها أنتم تقولون لنا الآن، أنكم أصبحتم تأخذون برأي آخر؟».

«لقد انتهى الأمر! بهذه العبارة، لخّص ستيوارت بيكر رأيه، وكان قد عاد بعد مغادرته وكالة الأَمن القومي في عام 1994 إِلىٰ مكتب المحاماة الذي يملكه ليختص بقوانين آلات التحكم التلقائي. وكان هناك من الناس من يعتقد أن الأمر كله مجرد تكتيك أخر للعرقلة تلجأ إليه الحكومة؛ وفي اللحظة الأخيرة يكشف واضعوا الأَنظمة النقاب عن خطة بحروف أنيقة لا تحتوي إِلاَّ على القدر اليسير من التغيير. وكان الأمر في تصورهم أشبه بلوسي تختطف الكرة من اللاعب تشارلي براون وهو يتهيأ لرميها، كذلك سوف تحول وكالة الأَمن القومي ومكتب التحقيقات الفيدرالي دون امتلاك القدرة على تصدير مفاتيح فعَّالة. ولكن بات من الواضح الآن أن حيز المناورة بات يضيق باطراد، قبل أن يسدّد تشارلي ركلته النهائية والقاضية.

والحق أن الحكومة وفت بوعودها هذه المرة. فكان مشروع الأَنظمة الأول يبدو كأنما يحتوي على قدر كبير من المحظورات والنواهي ينبغي الالتزام بها قبل منح برنامج تشفير قوي استثناء «تلقائياً»، لكن المسودة الثانية انطوت على تفهم أفضل بفضل المعارضة اللبقة إنما الحازمة أيضاً من طرف جماعة جودلات ـ لوفجرن والصناعة. حقاً أن القانون لم يكن مثالياً، إِلاَّ أنه كان واضحاً بما يكفي لطمأنة حتَّى المهووس إِلىٰ أن هذه المُنتَجات في طريقها إِلىٰ التصدير إِلىٰ الخارج. ولم يعد طول المفتاح إن كان معيارياً من 56 بت، أَو حتَّى 64 أَو 80، أَو 128، يعتبر سلاحاً قاتلاً.

لقد صار التشفير رسمياً مباحاً: صار التشفير العام صديقاً لنا.

بعد أيام قلائل من دخول الألفية الجديدة، تحين الذكرى العاشرة

للاجتماع السنوي، الذي تقيمه شركة آر إس إيه، لموضوع الكريبتوجرافيا، وبات الحضور يشغلون كافة الفنادق الفخمة في سان فرانسيسكو، أما مكان المؤتمر في هذه السنة فهو مركز المؤتمرات في سان خوسيه. لقد غدا اليوم، سوقاً ضخمة لبرامج الشيفرة وتقنياتها وله برنامج للندوات التي تدور على خمسة مسارات وعدد الحضور يربو عن الألف.

وقد دأب منظمو المؤتمرات أن يتناول أحد الخطابات الرئيسة التطور أَو سواه في الكريبتوجرافيا في المجال السياسي. وكان المؤتمر يجري وكأنما هو أشبه بمسرح الكابوكي (الياباني)، أبطاله ممثلون مفجوعون من عالم التجارة أَو الجامعات أَو عالم الحريات المدنية يشكون من عسف الحكومة. وقد تجد في المؤتمر مندوب عن الإِدارة سيء الفأل مساعد للمدعي العام، محام من وكالة الأَمن القومي، مستشار في سياسة التكنولوجيا يتأرجح على ساقيه، وتسمع هذا أَو ذاك يحاضر في جمع قاس عن التوازن الذي يعجز عنه الوصف بين السرِّيَّة والأمن القومي، ولعله يثير في مستمعيه أسباب الثورة بقول أساء اختيار موقعه مثل «لو كنتم تعلمون ما أعلم» في رد على أسئلة لا بد أن تكون مشحونة بالنقمة. ولكن الأمور كانت تختلف عما عهدها رواد المؤتمر في السنوات السابقة. فقد وجد الحضور جيم بيدزوس يتقدم من منصة المحاضر وبيده زجاجة يقدم الشمبانيا لأعضاء الندوة من وزارة العدل، ووكالة الأَمن القومي، وهو يقول انتهى القتال وفاز جماعتنا.

وكان بيدزوس قد انتهى من التفرغ للعمل يومئذ، ومرد بعض السبب إِلىٰ انتقال ملكية الآر إس إيه داتا سيكيورتي إِلىٰ شركة في الساحل الشرقي تعمل في مجال أمن الحواسب تدعى سيكيوريتي داياميكس. (وكانت الشركة المالكة الجديدة قد قرَّرت قبل عدة أسابيع من كانون الثاني/ يناير تغيير اسم الشركة فأصبحت آر إس إيه سيكيورتي، وكانت قيمة الصفقة حوالى 300 مليون دولار، وبلغ نصيب بيدزوس منها 40 مليون دولار. وهناك من يذهب إِلىٰ أن هذا هو

الرقم المعلن، أما في الحقيقة فلربما كان أعلى من ذلك، أو قد تكون شركة آر إس إيه استطاعت انتزاع حصتها البالغة بليون دولار بعد أن نجحت في برنامج الإدخال والمعالجة والإخراج على الإنترنيت لولا فضّ شركة ببليك كي بارتنرز على النحو المشين، حين اشتعلت الدعاوى بين آر إس إيه داتا سيكيوريتي وشريكتها سايلينك. فقد ضاق القوم في سايلينك بالشراكة القائمة وأزعجهم أن يحول الاتفاق الأساس دونهم واستثمار تكنولوجيا الخوارزمية «رسا» في مُنتَجاتهم؛ بل ولقد ذهبوا إلىٰ حد الاعتراض، على براءة ملكية معهد ماساتشوسيتس للتجديدات التي أتى بها رايفست ورفيقاه. (وهذه دعوى غريبة نظراً لأن سايلينك كانت تنال حصة من عائدات تلك البراءة، عن طريق ببليك كي بارتنرز). وفي غضون ذلك أزعج بيدزوس وزميليه أن تكون سايلينك قد طورت مُنتَجاً أساسه الخوارزمية «رسا» لصالح مصرف التصفية العالمي سويفت SWIFT. ولقد تمّت تسوية هذه الدعاوى في النهاية في أواخر عام 1996 بمعونة قاض فيدرالي. وكان أن ادعى كلا الطرفين الفوز في هذه التسوية المعقدة (لاحظ بيدزوس أنه لم يبرز في الدعوى أدلة تثبت أن شركة آر إس إيه خالفت قواعد السلوك السليم في تصرفاتها)، إلاّ أن الدعوى استنفذت الكثير من الطاقة من الطرفين ـ فيما كانت براءات الملكية الفكرية، تقترب من تاريخ الانتهاء).

ولقد ظن بيدزوس بعيد بيع الشركة، أنه سيكون أسعد حالاً إن تقلصت علاقته بها. وكان قد انتقل للإقامة يومذاك في قصر بناحية مارين كاونتي، واشترى مجموعة من سيارات بي أم دبليو الأنيقة ويتدرّب على عزف الجيتار الأصيل، ويقود أسطوله الصغير من الطائرات وأخذ بشراء الأسهم حتَّى أصبحت تملأ حقيبة بكاملها. ولقد أفاد من استثماراته حتَّى بات من أصحاب الملايين، كانت قيمة حصته الشخصية في شركة فيري ساين للشهادات الرقمية وحدها (وهو أحد مؤسسيها) تزيد على ما حصَّل من بيع شركة الآر إس إيه (تزيد قيمتها اليوم عن 100 مليون دولار). أما عمله الآن فهو ما يشبه السفير

المدافع عن قضية التشفير التجاري، ويظهر بصورة أساسيَّة في المؤتمر السنوي.

كان ديفي ما يزال يحضر المؤتمر، طبعاً، وشعره مرسلاً كعهده، ولحيته المهيبة كما عُرف بها، وتشخص إليه الأنظار في بذته الأنيقة المفصلة. ومع أنه لم يكن ثرياً بمعايير وادي السيليكون فإن بضعة الملايين من الدولارات التي كسبها من أسهمه في شركة الآر إس إيه جعلته في وضع مريح جداً. وقد ظل هو وماري فيشر على عهدهما عاشقين، وإن تقلصت مجموعتهما من الحيوانات الأليفة إلىٰ كلبين وحسب من الكلاب التيبتية الضخمة.

ولقد حضر المؤتمر أيضاً، رايفست وشامير وأدليمان. وكان رايفست قد غدا رجلاً ذا لحية غزاها الشيب، مهيباً وقوراً، وما زال يعمل بالتدريس في معهد ماساتشوسيتس، سوى أنه بات ثرياً بفضل ما يملك من الأسهم في شركة الآر إس إيه، وما انقطع يقدم أبحاثاً أصيلة في مجال التشفير. أما شامير فكان أكثر نشاطاً في العمل في هذا الحقل، يبحث عن كل جانب وجديد بدءاً من أَنظمة النقود الرقمية في تسديد المدفوعات الصغيرة إلىٰ كومبيوتر جديد قادر على تحليل الأعداد الكبيرة. ولكن لين أدليمان كان قد ابتعد عن التشفير والتفت إلىٰ بحوث تجمع بين الرياضيات وعناصر الكيمياء العضوية، مثل حواسب الأحماض النووية.

وكان هناك بعض الشخصيات البارزة في الكريبتوجرافيا، والمناضلون في هذا الحقل الذين تخلفوا عن حضور المؤتمر في سان خوسيه. فلم يجد رالف ميركل، الوقت لاستلام جائزة الآر إس إيه لمساهماته الهامة في هذا الحقل، وقد شغله عن استلامها عمله في مخابر شركة زيراكس بارك في حقل تكنولوجيا الجزئيات فحال دون وحضور الاحتفال. كذلك كان راي أوزي منهمكاً في تطوير أول مشروع كبير له منذ برنامج نوتس: وقد قدر له أن يحصل على إجازة تصدير مفاتيح رسا، بطول 2048 بت، و258 بايت، (نعم بايت ـ أي ثمانية

إضعاف البت!) آر سي ـ 4 ـ بعد خمسة عشر عاماً من احتكاكه الأول بوكالة الأَمن القومي. ثم، بالمناسبة، إجازة تصدير لمعيار معالجة البيانات العادي القديم، أيضاً.

وهناك، بعد، ديڤيد تشوم المسكين الذي حُرم من الظهور تحت الأضواء. ولو كان حضر، فلربما رأى الكثير من الأمور التي تستهويه. فقد كانت الإشارات تزداد إلىٰ حلول للشيفرة كالتي يقدمها تشوم كترياق لبث المعلومات الشخصية، وهو أمر غير مرغوب. فكان هناك شركة كندية تبرز منتجاتها في المعرض المرافق للمؤتمر، وتعرف باسم المعرفة الصفرية Zero Knowledge؛ وقد استطاعت هذه الشركة امتصاص الملايين لاستثماراتها، في مشروعها «المُعمِّي» Anonmizer، وهو عبارة عن موقع على الشبكة يسمح للناس بالتجول في الشبكة دون أن يخلفوا آثار أقدام رقمية وراءهم.

ومع أن يولف هيلسينجر، لم يغادر فنلندة لحضور المؤتمر فقد ظلت آراؤه تنتشر. ففي الاجتماع الشهري لزعران الشّيفرة والذي عُقد في عطلة نهاية الأسبوع السابق للمؤتمر دار النقاش المعهود في هذه الاجتماعات وكان موضوعه ظهور جيل جديد من مخدمي البريد، ويعرفون بالماكسيماسترز»، ويستخدمون تقنية محسّنة تيسر استخدام الرسائل المشفرة المغفلة عبر الإنترنيت إنما بالغة الصعوبة يشق عل الحكومة قراءتها كل المشقّة.

غير أن فيل زيمرمان استطاع، على كل حال حضور المؤتمر. وكانت الحكومة قد أسقطت دعواها في 11 كانون الثاني/ يناير 1996 ضده والمستهدف الآخر كيلي جوين. فأقامت زوجة زيمرمان حفلة بمناسبة «إفلات فيل» في مركز السلام في جبل روكي. ولم يمض طويل وقت حتّى قرّر زيمرمان الانتقال إلىٰ وادي سيليكون لينشئ شركة باسم منتهى السرِّيَّة Pretty Good Privacy, Inc لإنتاج البرمجيات التجارية. (كانت شركة الآر إس إيه قد ادعت على الشركة الجديدة ومقاضاتها لانتهاكها حقوق الطبع، وتمّت تسوية الدعوى في النهاية، وكان على

شركة بي جي بي دفع العائدات المترددة والمعتادة عن قواعد إرسال المفتاح العام). بيد أن الشركة لم يقيض لها الاستمرار طويلاً. والحق أن زيمرمان وهو الذي لا يستطيع، كما يقر بنفسه، ضبط دفتر الشيكات، سلم عمليات شركته لرجال أعمال، لتقويم وضع شركته، فأفلحوا في تدقيق حساباتها البالغة ملايين الدولارات. ثم توسعت أعمال الشركة الجديدة وضمت إليها شركات أخرى وشرعت تشارك بأجنحة تخطف الأنظار ببهائها في المعارض، وأخذت بخطة طموح لتتحول إلىٰ خدمة سرية كاملة عملاقة. وكان أن جرى بيع الشركة وقد شارفت الإفلاس إلىٰ شركة أمن حواسب شخصية راسخة تدعى نيتورك أسوشييتس، وظل زيمرمان يعمل في الشركة باعتباره رئيس برنامج بي جي بي، بيد أن مساهمته لم تكن في مجال تطوير برمجيات بقدر ما تكمن في مكانته رمزاً حياً للكريبتوجرافيا القوية. وبهذا الدور الرمزي حضر زيمرمان مؤتمر رسا 2000، في حفل أقامته نيتوورك أسوشييتس في الليلة الثانية من تلك المناسبة، حين وقف وأمامه لوحة مفاتيح الكومبيوتر وقام باستعراض كبير بتنفيذ نقل ملف بواسطة نقر الفأرة انتقلت معه نسخة من برنامج «منتهى السرِّيَّة» إلىٰ الخارج. وكانت الحكومة، قد أرادت أن ترمي به قبل سنوات قلائل في السجن للعمل عينه.

ولقد عقدت عدة جلسات في مراحل أخرى من المؤتمر ركزت الجهود التي ترعاها المؤسَّسة القومية للمعايير والتكنولوجيا لاختيار خليفة لمعيار تشفير البيانات. فعلى العكس من عمليَّة اختيار معيار تشفير البيانات الذي تم وراء الأبواب المغلقة، للحفاظ على سرِّيَّة مبادئ التصميم، كان طرح معيار تشفير البيانات المتقدم في إطار مسابقة يعلن اسم الفائز فيها في عام 2001. وهنا لا تقتصر العلانية على الخوارزميات وحدها بل وتسري على مقومات التصميم ذاته، وكل ما تطلبه مؤسَّسة القومية للمعايير والتكنولوجيا هو أن يكون المعيار الجديد أقوى من سابقه معيار تشفير البيانات، على ألاّ يقل طول المفتاح عن

128 بيت. وكان من الصعوبة بمكان أن يُطلب فرض قيود شديدة على تصدير الخوارزميات، نظراً لأن أكثر من نصف الخوارزميات المشاركة في المسابقة كانت من وضع كتّاب شيفرة يقيمون خارج الولايات المتّحدة.

كان قد مضى أكثر من عشرين عاماً منذ أن طلع هويت ديفي باكتشافه، والحق أن الأمر استغرق من الوقت ما جعل سلسلة براءات الملكية الفكرية بما في ذلك المفتاح العام وخوارزمية رسا تقترب في غضون شهور قلائل من بداية القرن الجديد من الانتهاء، ومع ذلك فقد وجدنا العصر الذي راود حلمه بدأ يطل أخيراً. ففي الكلمة الهامة التي ألقاها أحد نوّاب رئيس مايكروسوفت، بعد كلمة بيدزوس، أعلن صاحبها أن النّظام الجديد، ويندوز 2000 وهو نظام لا ريب أن أشكالاً منه، سوف تجد طريقها إِلىٰ كل كومبيوتر خاص تقريباً في القرن الجديد سوف يكون مزوداً بنظام تشفير من 128 بيت، ومعه ترخيص بالتصدير من الحكومة. وكان الكومبيوتر آبل، قد شرع يحمل نظام تشفير قوي في نظام تشغيله الجديد.

وكان نظام التشفير، قد أصبح أساسياً في كل متصفح في شبكة ويب، بما يتيح النقل الآمن لأرقام بطاقات الائتمان والمعلومات المالية. والمقدر أن تبلغ قيمة الأموال المتداولة بهذه الطريقة، في العام 2000، ما يزيد عن 80 بليون دولار ـ ويقدّر أن يرتفع الرقم في النهاية إِلىٰ التريليونات، ونكون نحن جميعاً تقريباً في حماية خوارزمية الرسا. وجدير بالذكر أنه سوف يصدر في وقت لاحق قانون يختص بالتوقيع الرقمي لقومي لتفسح الطريق أخيراً لتجاوز العقبات التي سبَّبها تباطؤ الإِدارة، في اتخاذ قراراتها سنة 1992. ولسوف يقوم الرئيس كلينتون بالتوقيع على القانون إِلكترونياً.

إن التكنولوجيا التي كانت محرَّمة ذات يوم، أصبحت الآن الدواء الشافي الجديد. كان التصور قد ذهب إِلىٰ أن التشفير، هو الحل لمشكلة نسخ الموسيقى والأفلام وتهريبها إِلىٰ الأسواق. فضلاً عن ذلك كان التشفير المادة

السرِّيَّة للأحاديث والمناقشات المحمية التي تدور جماعة من الجماعات وتجري في «شبكات خاصة تقريباً»، وهذا اتجاه تجاري هام يسمح بعقد المؤتمرات عبر الشبكة، دون أن يخترقها متلصّصاً أَو راصداً من الخارج. كذلك سوف يوفِّر التشفير السرِّيَّة لسجلات المرضى، فلا يمكن الاطلاع عليها إِلاَّ بامتلاك المفاتيح السرِّيَّة لمغاليق الملفات. ومن المتوقع، بعد، أن تصبح برامج التشفير عنصراً أساسياً في الجيل التالي من الإنترنيت، حيث سيكون لنا أن نتواصل مع كومبيوتر غير شخصي وأدوات تتراوح بين الكومبيوتر الشخصي والهواتف إِلىٰ أدوات المطبخ. ولسوف يكون كل ما يحيط بنا سلكياً ولاسلكياً، والتشفير، شبكة الأمان التي تضمن لنا السرِّيَّة.

وإذا شئنا الدقَّة، لقلنا أن الأثر الثوري لكل هذا، سوف يتسرَّب ويشيع خلسة بعيداً عن الأرصاد. فمئات الملايين الذين يستخدمون المستعرضات على الشبكة وأنظمة التشغيل لم يكونوا يدرون بهويت ديفي والآخرين، بل إنهم غدوا قادرين على إعجاز ثريسميوس السراني الذي عاش في القرون الوسطى وإدهاش فيجينيه الساحر صاحب المفتاح الذاتي، وحمل هورست فايشتل مبتكر لوسيفر على الابتسام، حتَّى بينما تقوم الآلات بعمليات التبديل وتفكيك وتركيب الشيفرة وإنجاز الصفقات التجارية بهدوء وسكينة. وإذن، لمَ كان هٰذا لاحقاً ولم ينجر كما توقع ديفي في وقت أقرب؟ والجواب أن السبب في ذلك أن الإنترنيت هو، الذي أتاح لهذا الإنجاز أن يحصل.

وإذن، هناك سبب وجيه، للاحتفال في مؤتمر آر إس إيه 2000. ولكن أولئك الذين يتساءلون عن السبب في سرعة التحول كانوا سيجدون الجواب الوجيز قبل غام من ذلك التاريخ، السبب ذاته والمكان ذاته والأشخاص ذاتهم، في مؤتمر آر إس إيه 1999. ولقد افتتحت تلك المناسبة بتصاعد أصوات جوقة كتاب مؤمني أوكلاند، حين ظهروا وملأوا المسرح وهم يرتدون جلابيبهم الزرقاء ويصدحون بأصواتهم على أنغام نسخة حديثة من الأنشودة الدينية: «ما

زلت انتظر ما أبحث عنه». كانت كلمات الأغنية، موضوعة قد حوّرت، لتبرز النضال الطويل من أجل شيفرة قوية تشيع بين الجمهور. حينما ظهر جيم بيدزوس ذاته على المسرح وهو في ذات الرداء قال في شهادته التي كان يتلوها بلهجة الواعظ أن السحب في انحسار وقوس قزح لا بد أن يظهر قريباً. وبشر بأنّه إن لم تعم فوضى التشفير فسوف تشيع الشّيفرة. فقد كان يدرك أن أحلامه المتصلة بالمفتاح العام طوال تلك الأعوام كانت أشبه بدفع صخرة إِلىٰ أعلى الجبل. ولكن المشكلة لم تكن في الحكومة أَو أَنظمة التصدير ذاتها. لقد كانت شيفرة المفتاح العام معجزة رياضية، إِلاَّ أنَّها نزلت علينا قبل الأوان. كانت يومذاك، قبل خمس وعشرين سنة، حلاً لمشكلة لم تظهر بعد تماماً.

كان ذلك أمر مضى وانقضى. وليس هذا هو الحال، في وقت نجد فيه كومبيوتراً، فوق طاولة مكتب ومتصلاً بالإنترنيت. ولا حينما يكون في كل حضن تقريباً أحد هذه الأشياء أيضاً. لا ولا حين بدأت الهواتف ترتبط بالشبكة العالمية، مع أجهزة التلفزيون بل وحتّى منصات ألعاب الفيديو. وليس قطعاً حين تستخدم أدوات اتّصالات الشبكة غير المرتبطة في نقل المعلومات بين الناس، بل وحتّى بطاقتهم الائتمانية وخاصة بطاقاتهم الائتمانية.

نظر جيم بيدزوس إِلىٰ مستمعيه وتعالى صوته الصدّاح معلناً: «قد وجدنا المشكلة للحل... وهي التجارة الإِلكترونية!».

الخاتمة: السر المكشوف

عوداً إِلىٰ الوراء، إِلىٰ عام 1969. كان هويتفيلد ديفي قد بدأ للتو يولي لكريبتوجرافيا تفكيراً عميقاً. ولم يكن مارتي هيلمان، بعد، يعمل في جامعة ستانفورد. ورالف ميركل ما زال في المرحلة الثانوية. وعالم الرموز ذات المستوى العالي ما زال ملكاً لوكالات الاستخبارات وتحت إدارتها. وقد ظل الأمر كذلك، حتّى ابتكر ديفي وهيلمان وميركل المفتاح العام. واكتشف رايفست وشامير وأدليمان تطبيقاته. وكانت أفكارهم المعجزة للعقل والتي أنهت احتكار الأشباح لهذا المجال، لا تزال في المستقبل البعيد.

لم يكن جيمس إلليز، من النوع الذي يسمي نفسه شبحاً. صحيح أنه عمل لصالح القيادة العامة للاتّصالات GCHQ، الصنو البريطاني لوكالة الأَمن القومي. لكنَّه يفضل أن يصف وكالته، وابنة عمها وكالة الأَمن القومي كذلك، بـ «المجتمع المغلق». لقد كان عضواً من جماعة تحفزهم الوطنية، والكبرياء، والحاجة البسيطة للمرتب لإعالة الأسرة. فإذا قدّر للمرء أن يحقّق إنجازاً رائعاً، فإن الاعتراف به يتم سراً، ضمن حدود المجتمع السري. وما أصاب جيمس إلليز من الألمعية والألق هو مثال بارز على هذا القول. فإلليز كان هو المخترع الحقيقي لكريبتوجرافيا المفتاح العام. وظل هذا الأمر مجهولاً لا يعلم به أحد واقعياً طوال قرابة الثلاثين عاماً.

لم يكن زملاء إلليز ليضعونه في عداد من يحتمل أن يأتوا بفتح يمكن أن يغير من قوانين مجالهم من العلم. وكان ينظر إليه على أنَّه قادر على الخروج بأفكار جيدة لكنَّه في أعماقه رجلاً حالماً. بل اعتقد بعضهم أنه على حافة الجنون. وقد وُلد في أستراليا وحين أصبح يتيماً ربَّاه جداه في شرق لندن. وفي الخمسينات وبعد تخرجه من إمبيريال كولدج، انضم إلىٰ القيادة العامة للاتِّصالات، في بلدة كوتسولدس في تشلتنهام. وكان إلليز يدرك أنه كان يدخل عالماً يُمنع فيه الاتِّصال مع العالم الخارجي بشأن عمله، الآن وإلىٰ الأبد. كان العمل هنا يعني أن يعمل المرء من أجل بلده؛ وعليه أن يضع أحلام الطموحات الشخصية والاعتراف العلني جانباً. وقد كتب إلليز قائلاً: «إن الأهمية القصوى للكريبتوجرافيا تتحقَّق بتقليص حجم المعلومات المتاحة للأعداء المحتملين إلىٰ أدنى حد. وإن المختصين في شؤون الكريبتوجرافيا المحترفين يعملون عادة في مجتمعات مغلقة لتأمين تفاعل مهني كاف لتحقيق مستوى رفيع من العمل والحفاظ على السرِّيَّة في الوقت ذاته».

قد يبدو في هذا شيء من العجرفة، لكن مهمة إلليز في الحقيقة لم تكن لتضعه وسط عالم المؤامرات الدولية. ويقول مالكولم ويليامسون، الذي سيكون له نصيب في هذه القصة بوصفه زميل المستقبل: «أعتقد أنه في بعض النواحي قد تمت تنحيته نوعاً ما. وعلى الأقل، كان انطباعي أنه لم يكن يعمل في أمور بالغة الخطورة ولم يعين فعلاً ليتولَّى المسؤولية في مشاريع كبيرة أَو شيء من هذا القبيل».

أما نيك باترسون الذي انضم إلىٰ القيادة العامة للاتِّصالات في أواخر الستينات، فيقول: «كان أقرب ما يكون إلىٰ أنموذج الرجل الإنكليزي غريب الأطوار: لطيف، غير منظم، يمشي متثاقلاً. وقد جرى بعض المدراء على التقليل من شأنه واعتبروه مجنوناً، لكنَّه كان رجلاً، لا ينضب معينه من الأفكار. والتي كان نصفها سخيفاً، لكن ربما كان نصفها الآخر مذهلاً».

وبالرغم من أن معظم الناس كانوا لا يرون فيه إلاَّ الرجل الغريب الذي اعتاد أن يعد قوته باستخدام النيسكافيه الممزوجة مع السكر والتي يضعها في مرطبان خاص به، لأنه كان يعتقد أن إضافة السكر بعد تذويب القهوة في الماء يجعلها أقل جودة. والعقبة الأخرى التي حالت دون الاعتراف بمواهبه، تمثَّلت في عدم قدرته على التعبير عن بعض رؤاه بشكل واضح. ويقول أحد زملائه: «كان أسوأ محاضر تقني صادفني على الإطلاق. وكان المستمعون يعتبرون أحاديثه محنة تامة. وعادة ما كان يبدأ حديثه بالاعتذار، بأنه طلب إليه تقديم عرض، لأمر لا يعرف عنه شيئاً، بعدئذ يمضي لمدة عشرين دقيقة في اتجاه غريب. ولكن عندئذ ـ وهذا هو السبب في حضور الناس لأحاديثه ـ ودون جعجعة يطرح شيئاً مذهلاً.

كان إلليز مستاء بعض الشيء، لأن واحدة من أهم أفكاره أهملت، فضاعت هباء. ذلك أن هيامه الشديد طوال حياته بتصاميم الراديو جعله يبتكر نوعاً خاصاً من الدارات السمعية التي تؤمن استقبالاً أفضل للموجات الصوتية. وحصل بالفعل على براءة اختراع لهذه الفكرة، وعرضت شركة أن تجرب وضعها في أجهزة الراديو التي تنتجها. لكن يبدو أن مهندسي الشركة، تنفيذاً لأوامر بتوفير المال عن طريق تقليص عدد المكونات قد أفسدوا تصميمه. وكانت النتيجة، أن استقبال الراديو لم يكن بالأمر الخارق الذي توقعه. فكان لهذه المهزلة أشد الوقع في نفسه وما انفكت تثير فيه أشد الألم.

في عام 1969، وكان إلليز في الأربعينات من عمره، ويعمل في قسم من الوكالة يدعى مجموعة أمن الاتِّصالات الإلكترونية، في منصب ربما كان الأنسب له: مجموعة من الباحثين ربما بلغ عددهم الستة يعملون على مشاريع طويلة الأمد. وكان قد عاد للإنضمام إلىٰ هذه المجموعة بوصفه كبير العلماء بعدما عمل لفترة في مكتب البريد، ومن المحتمل أنّه كان يساعد في مسائل أمنية. ووجد نفسه الآن يعمل على مشكلة اعتقد معظم الناس أنها عصية على الحل.

في الستينات، كانت المؤسَّسة الاستخباراتية، قد بدأت للتو في التفكير ملياً في الثورة في الكومبيوتر، والتقنيات اللاسلكية، وما تلا ذلك من حاجة ملحة، لتأمين الحماية لاتِّصالات الحكومة التي كانت تجري عبر هذه الأقنية. لكن بينما غدت الأَجهزة التي تقوم بالتشفير أرخص ثمناً، فإن جزءاً واحداً من العمليَّة لم يطرأ عليه تغيير جذري منذ الحرب العالمية الثانية. وكانت هذه وسائل توزيع وامتلاك المفاتيح الكريبتوجرافية. وكانت القيود الضرورية لحماية هذه المفاتيح بمثابة عنق الزجاجة: فكل شخصين يريدان الاتِّصال سراً، كان لا بد لهما من توليد مفتاح سري جديد من أجل هذه المحادثة بالذات. وكان الآلاف من الناس في تلك الحلقة السرِّيَّة؛ وذلك يعني حرفياً ملايين المفاتيح للتحرّك بأمان وحماية. وكانت المشكلة هي نفس المشكلة التي ستزعج هويت ديفي بعد حين: تلك التعقيدات المزعجة جداً، والأخطار الأمنية الناجمة عن إِدارة هذا العدد الهائل من المفاتيح.

كانت مشكلة صعبة، وبالطبع لم يتوقع أحد من جيمس إلليز أن يأتي بحل لها. فبعد كل شيء، كان ثمة قواعد معينة في الكريبتوجرافيا، تبدو راسخة رسوخ قوانين الفيزياء. وأي قانون مؤكد، أكثر من ذلك الذي يقول بوجوب عدم وضع المفاتيح السرِّيَّة المستخدمة في تشفيرالاتِّصالات، في موضع يمكن للدخلاء اعتراضها؟ لكن إلليز، وفقاً لزميل آخر يدعى كليفورد كوكس: «كان من ذلك النوع من الرجال الذين مهما تكن المشكلة التي تعطيها لهم يبدأون بتحدي الفرضيات الأساسيَّة، وغالباً ما يثيرون أسئلة تشير إِلىٰ بطلان الفرضيات التي كنت تعمل عليها ـ فرضيات ربما كانت تمنعك من بلوغ الحلول». وفي محاولة حل مشكلة إِدارة المفاتيح، تجد أن الكريبتوجرافيين بأجمعهم تقريباً يستبعدون أي حل يتضمن إرسال رسائل آمنة عندما لا يكون أسلوب التشفير معروفاً للمتلقي المحتمل فحسب، بل كذلك كل إرسال يفترض به أن يكون متاحاً للمتطفل كما هو للمتلقي المعني بالرسالة، بما في ذلك بث مادة المفتاح.

حتَّى إلليز، شكك بإمكانية ذلك. وكتب لاحقاً: «كان واضحاً للجميع وأنا منهم، أن الاتِّصال الآمن مستحيل دون مفتاح سري، أَو معرفة سرِّيَّة أخرى ما، أَو على الأقل طريقة ما يكون المتلقي فيها، في وضع يختلف عن وضع المعترض. وبعد، إذا كان المتلقي والمعترض في وضعين متماثلين، فكيف يمكن أن يكون أحدهما قادراً على تلقي ما لا يستطيع الآخر أن يتلقاه؟ وهكذا لم يكن هناك حافز للبحث في أمر من الواضح أنه مستحيل».

إلاَّ أن الحافز، سرعان ما سيتولد لدى إلليز. فقد كان ثمة ورقة بحث مغفلة التوقيع دُفنت منذ زمن بعيد في جبل من المواد السرِّيَّة المكدسة داخل حدود عالم الظلام. كانت الورقة تصف مشروعاً لشركة بل للهاتف في الأيام الأخيرة للحرب العالمية الثانية، وسرعان ما صنف بين الأعمال السرِّيَّة المحظورة ثم أصبح في عالم النسيان. وكان هذا جزءاً مما يسمى المشروع سي 43 C 43، وهو تجربة بدائية لكنها مبتكرة في التشفير التماثلي للصوت. ولشرح هذا نفترض أنَّك أردت إرسال رسالة عبر خط الهاتف ويراودك شك بأن شخصاً ما يسترق السمع. فكيف تستطيع إبقاء الرسالة آمنة؟ لقد افترض العالم المغفل الاسم في شركة بل أن على المرء الذي يريد تلقي الرسالة أن يضيف ببساطة ضجيجاً إِلىٰ الخط. فعندما يتم إرسال الرسالة فستختلط مع الضجيج بحيث أن مسترق السمع لن يسمع سوى كلاماً غير مفهوم. لكن المتلقي الذي يعلم على وجه الدقة كيف تولد هذا الضجيج، قد يستطيع أن يطرح هذا الضجيج من الإرسال ويحصل في النهاية، على الرسالة الأصلية غير المشفَّرة.

كان مشروع سي 43 عديم الجدوى، لأسباب تتصل بالكريبتوجرافيا الحديثة، منها أن النموذج كان تناظرياً بينما الناس الآن يستخدمون الاتصالات الرقمية. إِلاَّ أن إلليز وجد هذا النِّظام مثيراً: لأن المرسل لن يقلق من وجود عدو محتمل يسترق السمع، حتَّى ولو كان الخصم يعرف كيف يعمل النظام. وقد أدرك إلليز أن الذي جعل ذلك ممكناً، أنه بخلاف الكريبتوجرافيا التقليدية،

جعل المتلقي في الواقع مشتركاً في عملية التشفير. وكتب إلليز: «كان الاتّصال المأمون ممكناً، على الأقل من الناحية النظرية، إذا اشترك المتلقي في التشفير».

هل يمكن لنظام كهذا أن يعمل مع كريبتوجرافيا رقمية واقعية؟ قرَّر إلليز أن جوهر الأمر هو مسألة هرطقة: هل بالإِمكان فعلاً، إرسال رسالة مأمونة مشفَّرة رقمياً، دون تبادل مسبق للمفاتيح. ووفقاً لروايته، أن ذلك السؤال قد عرض له في فراشه ذات ليلة. وما هي إِلاَّ دقائق معدودة، حتَّى حصل على الجواب:

نعم.

فبينما كان جالساً هناك، في الظلام في غرفة نومه في تشيلتنهام، حصل على البرهان على القضية. وكان الاسم الذي أطلقه على المسألة يجسِّد التناقض: التشفير غير السري.

كانت خطة إلليز تتمركز حول مجموعة من ثلاثة تحولات رياضية. يستخدم المتلقي ـ ولتكن أليس ـ اثنان منها والمرسل (أهلاً ببوب مرة ثانية) سيستخدم الثالث. وفريق ثالث غير مرحّب به، ولتكن إيف. هي المعترض المحتمل والتي لديها كذلك القدرة على الوصول إِلىٰ هذه التوابع (الدوال)، لأنَّها في هذا السيناريو معلومات علنية/ عامة. تبدأ العمليَّة بعمل حاسم، أَوصى به لإلليز مشروع سي 43: يشترك المتلقي المحتمل للرسالة في عمليَّة التشفير. تبدأ أليس بتوليد عدد كبير تم اختياره عشوائياً، وهذا في الواقع، مفتاح سري لا يحمله أحد سواها. ثم تقوم كذلك عن طريق تنفيذ تابع رياضي معين، لتحويل المفتاح إِلىٰ عدد مختلف. ثم تقوم بإرسال هذا العدد الجديد إِلىٰ بوب.

إن هذا العدد الجديد هو النظير لما سيطلق عليه ديڤي وهيلمان فيما بعد، المفتاح العام. ولما كانت الدالة (التابع) تتميز بخاصية هامة أنه لا يمكن حسابها

بطريقة عكسية، لذلك حتَّى الذين لديهم هذا العدد الثاني غير السري، ويعلمون أي تابع أنتجه، لا يستطيعون القيام بحساب عكسي لاكتشاف العدد السري الأول. فهذا سيبقى معروفاً لدى المتلقي أليس وحدها.

والآن ولما كان لدى بوب هذا العدد غير السري، فإنه يستخدمه مع تابع آخر، لتشفير الرسالة التي يريد إرسالها لأليس. ثم يرسل الرسالة المشفَّرة لأليس. فكيف تعيد أليس الرسالة إلىٰ شكلها الأصلي كنص واضح بسيط؟ مع التابع الرياضي الثالث، تستخدم مفتاحها الأصلي السري بشكل أساسي لنزع التشفير عن الرسالة. ويمكن الآن لأليس، أن تقرأ الرسالة. في حين أن إيف لا تستطيع أن تقوم بشيء سوى أن تصرّ بأسنانها غيظاً.

في الواقع، أن المفتاح غير السري، يعمل مثل ضجيج الخط في مشروع سي 43: فبالرغم من أن أي متنصّت يمكنه سماع الضجيج على الخط، فإن المتلقي وحده يعرف كيف تم توليد الضجيج (هذه المعلومة هي المعادل للمفتاح السري)، وهكذا فالمتلقي وحده يمكنه عزل الضوضاء (أو في هذه الحال أداء الدالة/ التابع المناسب) لإعادة الرسالة المشفَّرة إلىٰ شكلها الأصلي الواضح. وحينما اكتشف إلليز خطة جعلت مبادئ المشروع سي 43 تتلاءم مع العصر الرقمي، فإنَّه قد غيَّر بالضرورة قواعد الكريبتوجرافيا. ولما كانت هذه المفاتيح غير السرِّيَّة لا تحتاج لحماية، فمن الممكن الحصول على اتِّصالات آمنة دون تدابير مسبقة. وكان هذا يعني أن الموظفين الذين يعملون في ذلك المجال لن يكونوا بحاجة لأن يزودوا مسبقاً بمفاتيح متماثلة، مفاتيح يجب عندئذ الحرص على حمايتها. لقد غدا الآن ممكناً التفكير باتِّصالات محمية على نطاق أكثر اتساعاً.

لم تكن المهمة الموكلة لإلليز، خلق ثورة في الكريبتوجرافيا، لكن عليه الآن التعامل مع احتمال أنَّه قد قام بهذه الثورة فعلاً. ومن المؤكد أن أساس هذه النظرية ذاتها ـ العنصر غير السري فيها ـ كان مناقضاً جداً في ظاهره لأعراف

الكريبتوجرافيا، لدرجة أن ضرب نظرية إلليز كان بالنسبة للبعض في القيادة العامة للاتّصالات بمثابة تأييد للنظام الطبيعي.

على أية حال، كان لا بد للفكرة من أن تُمحَّص. وفي شهر تموز/ يوليو 1969، تم إرسال مسودة بحث إلليز إِلىٰ شون وايلي وهو كبير المختصين بالرياضيات في القيادة العامة للاتّصالات لدراساتها، فمن المؤكد أن مجموعة الرياضيين، أَو ربما رئيسهم نفسه، لا بد أن يجدوا خطأ قاتلاً في هذا النِّظام. وقد استغرق إعلان النتائج أشهراً عدة، لكن قبل عيد الميلاد من تلك السنة، كتب وايلي خلاصة نتائجه: «للأسف، لا أستطيع أن أجد أي خطأ فيه».

لكن عالم الرياضيات، أشار إِلىٰ أن إلليز قد جاء ببرهان فقط، على أن مثل هذا النِّظام يمكن أن يوجد ولم يأت بالنِّظام نفسه. وما كان مفقوداً هو الوسائل لضمان أن ثمة طريقة آمنة لتوليد مفتاح غير سري (مكشوف) من المفتاح الخاص الأصلي، ذلك أنَّك كنت بحاجة لأن تتأكَّد من أن أمثال إيف في العالم، الذين بعد كل شيء سيكون بإمكانهم الوصول إِلىٰ المفتاح المكشوف، لكن لن يستطيعوا عكس تلك العمليَّة الأولى وكشف المفتاح السري. وكان إلليز قد حدس مجموعة من جداول البحث التي ستقوم بعدة حسابات للتشفير وفكّ التشفير، لكنَّه لم يأت بالتوابع (الدوال) المحددة ذاتها. وإِلىٰ أن تم اكتشافها ـ فإن الشك بإمكانية هذا قد انتشر بسرعة ـ ولم يكن يُنظر إِلىٰ التشفير غير السري إِلاَّ باعتباره شذوذاً نظرياً طريفاً، ولا شيء سوى ذلك.

يقول كليفورد كوكس: «كانت النتيجة أن سمعنا، إن هذا رائع بالفعل، إنه عمل عبقري، في منتهى الذكاء، ولكن كيف نستطيع الإفادة منه؟».

عندما دون إلليز مشروعه في كانون الثاني/ يناير عام 1970، لم يقم بتغليف هذه المشكلة وتزويقها ظاهرياً. لكن المعرفة بمضامين فكرته لم تكن تعوزه. ذلك أن عنوان البحث الذي نشر داخلياً ـ كان سرياً بالطبع ـ «إمكانية التشفير غير السري الآمن» وقد كتب في الخاتمة «من الضروري التمييز بدقة بين

الواقعة والرأي، أي بين ما تم إثباته بالفعل وذلك الذي يرجح أن يبدو كذلك. والقيام بهذا أمر صعب خاصة في هذه الحالة ذلك أننا أثبتنا أمراً، يبدو لمعظم الناس أنه بطبيعته مستحيل». وفي الحقيقة، أن المفهوم ليس مستحيلاً لأنه أثبت «بدقة متناهية» أن مشروعه كان «مقبولاً نظرياً».

كان ثمة خطوة واحدة لا بدّ منها لإنتاج وسائل ثورية للتشفير، وهي إيجاد الدوال (التوابع) الرياضيَّة المناسبة. ولم يكن هذا بالأمر السهل. ذلك أن إلليز منذ أن بدأ بحثه كان قلقاً بشأن مهاراته الرياضية التي لم تكن ترقى للمهمة. (فقد تدرب ليكون مهندساً). وبالرغم من المزايا الواضحة التي يمكن للنظام غير السري أن يقدمها، إلاَّ أن القيادة العامة للاتِّصالات لم تعتقد أنه من المجدي رفده بمزيد من الأدمغة لمساعدته في البحث. ومع ذلك، وفي أوقات مختلفة وعلى مدى عدة سنوات تالية، كان بعض الكريبتوجرافيين لدى مجموعة أمن الاتِّصالات الإلكترونية يطَّلعون على البحث ويعملون على إيجاد بعض الحلول الممكنة. وفي عام 1971 اهتم رئيس العلماء المعين حديثاً بالمشكلة وعيّن بعض الأشخاص ليحاولوا إيجاد حل لها. لكن البحث في التوابع الغامضة أفاد هؤلاء بأن تكون لديهم بالنتيجة فهم لمميزات مثل هذه الأمور، إلاَّ أن محاولاتهم لم تجد نفعاً ولم توصلهم إلىٰ حل للمعضلة. وهذا أدَّى إلىٰ رجحان كفَّة الذين يصرون على أن المفهوم برمته أمر مستحيل.

ليس معروفاً إلىٰ أي درجة، كانت وكالة الأَمن القومي قد ساهمت في العملية، إذا كانت قد شاركت على الإطلاق، منذ أن تعاون الرؤساء السابقين في أيام بليتشلي، قامت القيادة العامة للاتِّصالات بإطلاع ما يسمونهم أبناء العم الأمريكيين على ما لديها من أسرار. لكن ليس هناك أي دليل على أن وكالة الأَمن القومي قد بذلت جهوداً في مجال التشفير غير السري في تلك المرحلة. وتشير الوثائق التي نشرتها القيادة العامّة للاتِّصالات إلىٰ أن العمل في هذا المجال كان مقتصراً على عدد من الكريبتوجرافيين العاملين لدى مجموعة أمن

الاتّصالات الإِلكترونية، الذين كان لديهم حرية الوصول إِلىٰ المشروع، وكان لهم اهتمام للخوض فيه. ولما كان بلوغ الحل يبدو أقل احتمالاً، فإن أعداد هؤلاء أخذت تتناقص.

وهنا بدأ دور كليفورد كوكس في القصة. ففي عام 1973، كان كوكس موظفاً حديث العهد في مجموعة أمن الاتّصالات الإِلكترونية. وهو ابن لأبوين من الطبقة الوسطى ـ كان والده محاسباً ـ وكان كوكس على قدر من الذكاء مكّنه من اجتياز امتحانات مدرسة مانشيستر الثانوية، وهي مدرسة تنافسية مستقلّة، ذات مكانة علمية راسخة. ثم التحق بكلية كينجز كوليج في كمبريدج، ليحصل على إجازة في الرياضيات. وتابع دراساته العليا لمدة سنة في أكسفورد، باحثاً في نظرية الأعداد. ويقول: «لم أكن أحرز تقدماً فعلياً». إذن فأين يعمل؟ وبالرغم من أنّه لم يكن يعرف كثيراً عن القيادة العامة للاتّصالات، ولا فكر جدياً في الكريبتوجرافيا على أنّها مجال عمله، إلاّ أنه كان يعلم أن الوكالة السرِّيّة كانت بحاجة إِلىٰ مختصين بالرياضيات. كذلك كان واحداً من أصدقاء الطفولة ويدعى مالكولم ويليامسون يعمل لدى القيادة العامة للاتّصالات. (عندما حقّقت الحكومة في طلب كوكس أبدى المحقّقون اهتماماً خاصاً بهذا الأمر، ربما خشية أن يكون في هذه المصادفة ما يريب) وهكذا دخل كوكس المجتمع المغلق، في أيلول/ سبتمبر عام 1973، وهو في الثانية والعشرين من عمره.

إن احتمال عدم نشر الأبحاث بصورة علنية ليطلع عليها من يشاء لم تزعج كوكس، إذ يقول: «لقد كنت سعيداً لهذا». فلن يكون هناك أي ضغط للتنافس مع عباقرة الهيئات الأكاديمية. ذلك أن افتقار أبحاثه عندما كان طالباً للنتائج قد قاده للاعتقاد بأن مساهمته ستنصب بصورة أكبر على الجهود العملية التي سيكرسها لحكومته.

بعد أن يتم توظيف الناس في القيادة العامة للاتّصالات، كان يعين لهم

مرشد خاص يتولى، حسبما يقول كوكس: «تعليمك، ويرشدك إِلىٰ ما تحتاج إِلىٰ معرفته». وكان معلمه يدعى نيك باترسون، وهو مختص بالرياضيات من كمبردج أيضاً. وكان أعجوبة في لعبة الشطرنج في مسقط رأسه آيرلندة، ولم يكن ليكبر كوكس سوى ببضع سنوات. وكان يتوقع له النجاح على الدوام. وفي عصر أحد الأيام أثناء تناول الشاي، وبعد حوالي شهرين من التحاق كوكس بعمله. أشار باترسون إِلىٰ فكرة إلليز. ولم يقدمها للشاب على أنَّها تحد، لتطبيق نوع جديد من الكريبتوجرافيا، ولكن على اعتبارها أقرب ما تكون إِلىٰ الأحجية. ويقول كوكس الذي يعتقد أن عدم اطلاعه على بحث إلليز كان ميزة: «لقد شرحها لي نيك بصورة رياضية جداً، من حيث الحاجة إِلىٰ دالة (تابع) لا تعكس وتتمتع بخاصية التشفير وفك التشفير». وهذا ما جعله يعالج المشكلة دون أفكار مسبقة. ولما كان قد أجرى أبحاثه في السنة السابقة، في نظرية الأعداد ـ مستخدماً الأعداد الأولية الكبيرة والمضاعفات ـ فمن المنطقي أن يستخدم تلك المعرفة لتطبيق نظرية إلليز، وكان الأمر كما كان يأمل».

وأضاف قائلاً: «أعتقد أنه كان مفيداً، أنني لم أكن مشغولاً بأي شيء، ذلك المساء». فقد عاد في تلك الليلة إِلىٰ الغرفة المتواضعة التي استأجرها في تشيلتنهام وتناول طعام العشاء الذي أعدته صاحبة البيت حيث ينزل عندها بين أفراد أسرتها، ثم جلس يفكّر. وبسبب السرِّيَّة التي تفرضها القيادة العامة للاتِّصالات في جميع الأمور المتصلة بعمله، كانت هناك حدود لا يملك تجاوزها. فلم يكن يسمح له بإحضار أي شيء إِلىٰ بيته من مكان عمله. وإذا كان يفكر ملياً في مشكلة تتصل بعمله أثناء وجوده في غرفته المستأجرة، لم يكن مسموحاً له أن يكتب أي شيء، ولا حتَّى ملاحظات على أوراق المسودة. فكان عقله الشيء الوحيد الذي يحمله معه. وقال: «لحسن الحظ، بدا أن الفكرة الأولى تعمل جيداً».

كانت الفكرة الأولى أكثر من مجرد جيدة ـ كانت رائعة. وقال كوكس:

«إذا كنت تريد تابعاً لا يمكن عكسه، فيبدو من الطبيعي لي، أن أفكر في مفهوم ضرب أعداد كبيرة جداً ببعضها البعض». واعتقد كوكس أن «المفتاح» السري سيكون في تطبيق عددين أوليين كبيرين، تولدهما المتلقية أليس فوراً، ويكون حاصل ضربهما هو المفتاح غير السري، وهو العدد الذي يعطى للمرسل بوب. (يمكن لبوب أن يجده في دليل موزع على العموم). ثم اكتشف كوكس صيغة رياضية بسيطة تمكن بوب من أن يستخدم العدد غير السري ليشفِّر الرسالة بطريقة لا يمكن لأحد أن يفك تشفيرها سوى الشخص الذي يعرف الأعداد الأولية الأصلية.

كانت الصيغة من الناحية الفعلية هي الصيغة ذاتها لما نطلق عليه الآن خوارزمية رسا. لقد أنتج كليفورد كوكس في ليلة واحدة، ما أعاد اكتشافه بعد ثلاث سنوات ثلاثة سرعان ما أصبحوا رياضيين مشهورين في معهد ماساتشوسيتس للتكنولوجيا واستغرق ذلك الإنجاز منهم أربعة أشهر من المحاولة والخطأ.

يتذكر كليفورد، أن أول إنجاز لمفتاح عام في العالم قد تم على الأرجح حوالي الساعة السابعة أو الثامنة. وقال لنفسه حينذاك «إن هذا لمثير للغاية». ثم اخلد إلىٰ النوم، بعد أن نظم الفكرة في عقله. ويقول: «عدت إلىٰ العمل في اليوم التالي وهناك دوّنت ما توصّلت إليه».

وضع البحث القصير على مكتب نيك باترسون وانتظر رد فعل معلمه. ويروي باترسون قائلاً: «لقد أصابني نوع من الجنون». ويعترف بأنَّه انتابه يومذاك الاهتياج الذي يعرف به الآيرلنديون واندفع مخترقاً الرواق ليصل إلىٰ مكتب أخصائيي أمن الاتّصالات الذي يبعد أربعين ياردة عن مكتبه، وفتح الباب على مصراعيه، وراح يصرخ قائلاً: «إن هذا أعظم اكتشاف كريبتوجرافي في هذا القرن». وذلك وسط ذهول الموظفين البيروقراطيين الرجعيين المنزرعين وراء مكاتبهم.

لكن هذا، على أية حال، كان رأي الأقلية. وحتّى كوكس شعر في ذلك الوقت، أن الأمر كان أقرب إِلىٰ حل ذكي لأحجية رياضية من أن يكون نقطة تحوّل بالفعل. ولما بدأ الأمر يشيع في مجموعة أمن الاتّصالات أن أحدهم قد وجد طريقة لتطبيق فكرة جيمس إلليز الغريبة، فإن أحداً بالطبع لم يعامل الأمر على أنه مثل عودة المسيح أو أي شيء من هذا القبيل. ويذكر كوكس: «كان الناس يقولون ها، ها هاكم طريقة، ونعم العمل».

يبدو أنه ما من أحد يذكر، لحظة سماع جيمس إلليز، عن الاكتشاف الذي قام به كوكس. يقول باترسون مخمناً: «أعتقد أن ذلك حدث في ذلك الصباح. لقد كان سعيداً جداً». لكن إلليز كان حذراً كذلك متخوفاً، ربما من أن القيادة العامة للاتّصالات لن تأخذ الفكرة بالجدية التي تستحقها. وإن كوكس نفسه لا يذكر أول لقاء له مع إلليز، الذي قدّر له أن يتعرّف عليه جيداً في الأشهر التالية.

حصل كوكس، على إذن لكتابة ورقة بحث عن فكرته، وذكر ذلك لصديقه مالكولم ويليامسون، (بالرغم من أن ويليامسون كان يسكن في نفس البيت الذي يسكن فيه كوكس، فإن المحادثة كان لا بد أن تحدث في مكان العمل. إذ كان تبادل الآراء في موضوعات تتعلّق بالعمل يحظر أن تتم خارج جدران القيادة العامة للاتّصالات). وكان هذا خطوة إِلىٰ الأمام نوعاً ما، لأنه كان من غير المألوف أن يقوم موظف جديد بتوزيع ورقة بحث بهذه السرعة بعد وصوله. وقد أثار الإعلان انتباه ويليامسون، فأصغى جيداً لشرح كوكس للمشكلة وكيف توصل إِلىٰ حلّها.

كان ويليامسون قد عرف كوكس منذ أن كان في الثانية عشرة من عمره. فهو الآخر كان طالباً في مدرسة مانشيستر الثانوية، وينتمي شأنه شأن صاحبه إِلىٰ أسرة من الطبقة الوسطى؛ إذ كان والده بائعاً لدى شركة نسيج. ولما كان كل من كوكس وويليامسون متفوقاً في الرياضيات، فقد قامت بينهما منافسة لطيفة، وإن لم تكن معلنة. كذلك فإن ويليامسون التحق بجامعة كمبردج حيث درس

في كلية ترينتي التي تفتخر، بأن نيوتن كان من بين خريجيها، ثم قام ببعض الأبحاث في الطبولوجيا، أثناء دراسته العليا في جامعة ليڤربول. وفي أحد الأيام راودته أمنية: بأن ينذر حياته لتعليم الرياضيات متى حصل على شهادة الدكتوراه. وكان في تلك الفترة يدرس صفاً من المهندسين وقد ثبط من عزيته أن أحداً من طلابه لم يستطع، أن يثبت أن الجذر التربيعي للعدد 3 هو عدد أصم. يقول: «لم أستطع أن أشرح لهم لماذا يجب عليهم أن يهتموا، ولم أكن مهتماً أنا الآخر بهذا الأمر. ولذا تساءلت: لماذا أقوم بهذا؟» وفي ذلك الوقت تقريباً شاهد إعلاناً تطلب فيه القيادة العامة للاتِّصالات مختصين بالرياضيات للعمل لديها. ودون أن يعلم كثيراً عن هذه الهيئة، استجاب للإعلان، ووجد نفسه موكلاً بمسائل الكريبتوجرافيا.

كان ويليامسون قد سمع بمسألة إلليز من قبل، إلاَّ أنه وجدها أقرب ما تكون إِلىٰ الهراء. كيف يمكنك ممارسة الكريبتوجرافيا وقد مررت المفتاح بشكل علني؟ وهكذا انطلق ليقضي على هذا المفهوم وعلى حد قول ويليامسون: «لدحض فكرة كليف».

كان ذلك بعيد العشاء، عندما بدأ ويليامسون، في غرفته، جهوده في الفحص والتدقيق. ويقول مفسراً: «إنّك تحاول تحويل مشكلة ما إِلىٰ مجموعة من المفاهيم العامة والأساسية جداً. كنوع من الامتحان الدقيق. ولم أستطع أن أثبت أن هنالك أي خطأ في ما عرض له».

لكن أثناء قيامه بهذه العملية، بدأ ويليامسون في التفكير في طرق مختلفة يمكن من خلالها لفريقين متعاونين فيما بينهما أن يمرّرا أعداداً جيئة وذهاباً ليصلا إِلىٰ مفتاح، مفتاح مشترك يكون مأموناً حتَّى ولو كان ثمة متنصت (شرير مثل إيف) يراقب كل خطوة في عملية التبادل. كان الوقت متأخراً من الليل عندما توصل إِلىٰ إدراك الفكرة، ويعتقد أنه ربما كان ذلك بعد ثمان أَو اثنتي ساعة من التفكير، ولكن في النهاية كان لديه خطته الخاصة، التي تتضمن

مجموعة معقدة من التبادلات، التي يقوم فيها كل فريق بانتقاء عدد عشوائي، ويجري عليه حساباً باستدخام صيغة يصعب عكسها، وأخيراً يصل كل فريق إِلىٰ مفتاح مشترك. ومن الناحية القانونية كان ويليامسون ممنوعاً من تدوين ذلك على الورق أثناء وجوده في منزله. طبعاً كانت الفكرة تصبح ملكاً للدولة، حالما تخرج من رأسه، ولم يكن ذلك ليزعجه. وفي ذلك يقول: عندما تكون قد توصلت إِلىٰ مفهوم صحيح، فلا يمكن أن تنساه. وكل شيء يتتابع منطقياً». مع ذلك وكما يذكر صديقه كوكس ساخراً، في صباح اليوم التالي، كان أول ما سجلته ذاكرة كوكس أن ويليامسون قد وصل باكراً إِلىٰ العمل.

وكان أول شخص أخبره عن اكتشافه ـ كما يقول ويليامسون ـ هو إلليز ذاته، الذي كانت معرفته به في ذلك الوقت ضئيلة. ولا يتذكر الكثير عن المحادثة، لكنَّه يتذكر في الأسابيع التالية: «لقد جعلني جيمس أرى الأمر أكثر وضوحاً. مع ذلك فإن عدم كتابة ويليامسون للعمل الذي قام به إِلاّ بعد شهرين، إنما كان مؤشراً لعدم الأهمية النسبية للمشروع من وجهة نظر القيادة العامة للاتِّصالات. (وقد أنهى مذكرته في شهر كانون الثاني/ يناير 1974؛ في حين أن عمل كوكس، يرجع إِلىٰ شهر تشرين الثاني/ نوفمبر 1973)، وبعد وقت قصير، ومزيد من المحادثات مع كلينتون خرج بفكرة أخرى نظمت المفهوم الأصلي. وكانت هذه تقريباً الصيغة الدقيقة ذاتها لما سوف يعرف لاحقاً باسم ديفي ـ هيلمان لتبادل المفتاح. أما فيما يتعلَّق بويليامسون، فبالرغم من أن البحث كان إِلىٰ حد كبير نتيجة لورقة البحث الأولى، فمن الواضح أنه شعر بأنه ليس في عجلة من أمره لتوزيع بحثه ضمن الدائرة. ويقول: كان أسهل بقليل. . وبالفعل لم يبد أن ذلك يمثّل خطوة كبيرة».

والآن، أصبح لدى القيادة العامة للاتِّصالات وسيلتان، لا وسيلة واحدة وحسب، لتطبيق بدعة إلليز. ولكن كما كانت تنتاب الوكالة الريبة من خطة إلليز الأساسية، فقد التزمت الحذر الشديد من هذين المشروعين. ويقول كوكس: «إن أول شيء أردنا التأكّد منه أنه كان مأموناً».

والغريب في الأمر، أن العامل الوحيد الذي كان ضد التشفير غير السري هو روعة مشروع كوكس والتطبيق الثاني لويليامسون. يقول ويليامسون: «إنه مغر وجميل، إلاَّ أن الأناقة لم تكن ما نبحث عنه سابقاً في أَنظمة التشفير. فهناك قاعدة أساسية تقول أن المشكلات المرتبة والأنيقة، لها حلول مرتبة وأنيقة، أما المشكلات الفوضوية فليس لها حلول مرتبة وأنيقة. والآن، معظم تصاميم الشيفرة فوضوية بشكل أساسي؛ إنها ليست مرتبة ولا أنيقة أَو رياضية. لذا نحن مرتاحون إِلىٰ حد كبير إِلىٰ أن الناس لن يكونوا قادرين على حلّها، ذلك أنّك حتّى ولو استطعت التسلّل إليها، فلن تقع فجأة على برغي سحري صغير بحيث إذا قمت بحله وجدت كل شيء ينهار. لكن في هذه الأمور المرافقة للمفتاح العام، فمما لا ريب فيه أنه من الممكن أن يوجد برغي سحري. ويمكن لطالب مجاز بالرياضيات أن يتسبَّب فعلاً بوقوع كارثة».

كانت القيادة العامة للاتّصالات، قلقة جداً بخصوص هذه المسألة، لدرجة أنَّها لم تكتف بالنظر في هذين المشروعين داخلياً دون أن تجد أخطاء متأصلة فيهما، بل خطت كذلك خطوة غير عادية بأن لجأت إِلىٰ بروفسور شهير من خارج المؤسَّسة يدعى آر. إف. تشيرتشهاوس وقدمت له العمليات الرياضية التي تقوم عليها فكرة كوكس وسألته إن كانت مأمونة. وخلص تشيرتشهاوس إِلىٰ نتيجة مفادها أنه طالما لم يكتشف أحد طريقة سريعة لتحليل الأعداد الكبيرة إِلىٰ عواملها ـ وهو شيء لم يستطع أي رياضي الاقتراب منه ـ فإن المشروع مأمون.

في النهاية وجدت القيادة العامة أن طريقة ويليامسون، هي المفضلة بين الطريقتين، لأن التوابع الخاصة بها كانت أسهل في التعامل معها من الأعداد الهائلة التي أتت مع مشروع كوكس الذي يقوم على أساس الضرب. ومع ذلك، اعتبر النِّظام غير عملي. ويشرح لنا كوكس ذلك بقوله: «كانت الآلات التي ستستعمل باهظة الثمن وبطيئة جداً. وتحتاج إِلىٰ عدة دقائق لتوليد [مفتاح].

ونظرنا في الظروف التي ستجد فيها فائدة الحصول على آلة، تستغرق وقتاً طويلاً لإنتاج [المفاتيح] وسرعان ما اعتقدنا أن التطبيقات كانت محدودة جداً، لتكون جديرة بالتعويم».

أما في داخل القيادة العامة للاتّصالات فإن الحكمة السائدة تغيرت من «مستحيل» إلىٰ «غير عملي». بالإضافة إلىٰ أن الكثيرين ما زالوا متخوفين من الجانب «غير السري» للمنهج. وذهب التفكير يومئذ إلىٰ كون هذا النوع الثوري الجديد من الكريبتوجرافيا ينطوي على نقاط ضعف دقيقة يصعب اكتشافها، نقاط ضعف يمكن للعدو استخدامها لاختراق النِّظام.

حتَّى مالكولم ويليامسون اعتقد أن المغامرة برمتها، كانت محفوفة بالمخاطر. وعندما كتب أخيراً النسخة المنقحة من المشروع الذي وضعه للمفاتيح، ذكر أن هذه التحفظات كانت السبب، وراء التأخر [في الكتابة] مدة سنتين. إذ كتب: «إنني أجد نفسي في وضع حرج. فبعد أن كتبت [بحثي الأول]، أصبح يساورني الشك في مسألة نظرية التشفير غير السري برمتها. والمشكلة أنه ليس لدي دليل على أن الطريقة... مأمونة حقيقة». ثم ينتقل لاحقاً إلىٰ الشكوى «أشعر بأنَّه لا بدّ من وجود عيب ما في أمن الطريقة. لكنني لا أستطيع أن أجد أي خطأ فيها، وسأكون ممتناً، إذا كان بمقدور أي شخص آخر العثور عليه».

وكان ذلك أمراً لم يقم به أحد. لكن القيادة العامة للاتّصالات توصلت بصمت في ذلك الحين إلىٰ قرار، مفاده أن تطبيق نظام المفتاح العام للتشفير لا يستحق الجهد الذي سيبذل من أجله.

في عام 1976، كان ديفي وهيلمان قد عرضا، طبعاً، ما توصلا إليه، أولاً في كانون الثاني/ يناير، (بعد أن وزعا مسودات غير رسمية قبل ذلك التاريخ)، ثم قدما النسخة المعدلة في تشرين الثاني/ نوفمبر تحت عنوان «اتجاهات جديدة في الكريبتوجرافيا». وتلاه بعد ذلك البحث المتعلّق [بخوارزمية] رسا

عام 1977. وقد حصل أصحابها على الشهرة، إن لم يكن على الثراء فوراً. لكن بسبب الأخلاقيات والقانون، لم يكن بمقدور العلماء في القيادة العامة للاتّصالات أن ينبسوا ببنت شفة، وظلوا صامتين عن الحقيقة.

واستناداً إلىٰ كوكس، أن جيمس إلليز، لما قرأ البحث الأول، الذي رسم الخطوط العريضة للفكرة دون اقتراح أي تطبيق لها، قال: «إنهم الآن حيث كنت عام 1969». وبالطبع فإن البحث الثاني لفريق عمل جامعة ستانفورد قد اقترح وسيلة للتطبيق، وهي مطابقة للحل الذي وضعه مالكولم ويليامسون. (ليس من الواضح ما إذا كانت أبحاث ديفي ـ هيلمان قد قادته إلىٰ كتابة ما اعتبره «خطوة صغيرة» ثانية في تطبيق البحث الأول، لكن بحثه يرجع إلىٰ آب/أغسطس 1976، بعد أشهر من البحث الأول المنشور لديفي وهيلمان). أما كوكس فكان قد ترك القيادة العامة للاتّصالات مؤقتاً للقيام بمهمة محددة في وزارة الدفاع، وكانت أول مرة يعلم فيها بالاكتشاف الأمريكي حين قرأ مقال مارتين جاردنر في منتصف عام 1977، ذلك المقال الذي وصف خوارزمية رسا التي كان قد اكتشفها قبلهم بثلاث سنوات. فقال: «لقد فوجئت».

من المؤكد أن الكريبتوجرافيين البريطانيين، كانوا في ذلك الوقت يتابعون نظراءهم، الذين يعملون خارج عالم الأشباح. ومن الواضح أنّهم شعروا بالفزع عندما علموا، في وقت لاحق من عام 1977، أن جامعتي ستانفورد ومعهد ماساتشوسيتس للتكنولوجيا، كانا يعتزمان الحصول على التوالي، على براءتي اختراع خوارزميات ديفي ـ هيلمان ورسا، اللتان تم ابتكارهما أساساً لدى مجموعة أمن الاتّصالات الإلكترونية. وهذا ما أثار غضب ويليامسون بشكل خاص.

ويقول: «حاولت أن أحمل القيادة العامة للاتّصالات، على منع براءة الاختراع الأمريكية. وكان بمقدورنا القيام بذلك، لكن الأشخاص في المراكز العليا لم يكونوا يريدون ذلك في الواقع. وأن براءات الاختراع قضية معقدة». وكان هناك، على وجه الخصوص، مسألة ما إذا كان بالإمكان الحصول على

براءة اختراع، وفق القانون البريطاني لأمر كان بالأساس عبارة عن خوارزمية رياضية، وكانت هنالك بالطبع مسائل أمنية أيضاً، إذ لم يكن مما يناسب القيادة العامة أن تدع غرباء يعلمون ما الذي يفكر فيه رجالها. كذلك يقول كوكس: «كانت النصيحة التي تلقيناها لا تزعجوا أنفسكم بهذا الموضوع». أما ويليامسون الذي لا يزال يعتقد أن رؤساءه قد جانبوا الصواب في هذه القضية، فيتذكر رئيس العلماء الذي أتى إليه أخيراً وقال: «لا، إننا لن نعمل على إيقاف براءة الاختراع».

والتزم عالم الظلال بالبقاء هادئاً.

وهكذا، فإن جبن وعزلة ما أطلق عليه إلليز، اسم «المجتمع المغلق» قد أدى إلىٰ فشل إبداعي: وبالرغم من انطلاقتها الجديدة فقد تخلت [القيادة العامة] كلياً عن فكرة المفتاح العام وسلمتها إلىٰ الغرباء الذين استخدموها لا ليبنوا مجتمعاً بديلاً فحسب، بل كذلك ليبنوا صناعة كاملة (كان أول منتج عرف بأنه استخدم تقنية المفتاح العام خرج من وكالة الأَمن القومي أو القيادة العامة للاتِّصالات هو الهاتف المأمون إس تي يو ـ 3 STU-III الذي أنتج عام 1987، بعد زمن طويل من نشر بحث ديفي وهيلمان. وكانت آر إس إيه داتا سيكيوريتي في ذلك الوقت في طريقها إلىٰ طرح حلول سهلة للتشفير).

بالإِضافة إلىٰ ذلك، فإن رجال الحكومة بإعراضهم عن فكرة كريبتوجرافيا المفتاح العام ووضعها جانباً، قد عجزوا عن رؤية بعض الجوانب الأهم في اكتشافهم. وكان من أهم تلك الجوانب الفكرة القائلة بأن أهمية كريبتوجرافيا المفتاح العام تكمن في قدرتها على إثبات هوية مرسل الرسالة (التوقيع الرقمي) بالإِضافة إلىٰ ما تتمتع به من خواص تشفيرية. والأكثر من ذلك، أن الوكالتين برفضهما التشفير غير السري بسبب بطئه الذي يجعله غير عملي، قد فوَّتتا ما اتضح أنه حل بسيط للمشكلة: استخدام خوارزميات غير سرِّيَّة مقترنة مع أنظمة تقليدية للمفتاح المتماثل. وحالما نشر ديفي وهيلمان بحثهما، فإن العقول

المبدعة في القطاع الخاص لم تستغرق وقتاً طويلاً لتستنتج أن في هذه الأَنظمة «الهجينة» يكمن مستقبل تقنيات السرِّيَّة.

كانت هذه واحدة فقط، من الابتكارات المبنية على المفتاح العام التي نشأت عن حرية النقاش التي شاعت في جو من الانفتاح. ففي هذا الجو طرحت أفكار مثل النقد الرقمي (المغفل أَو القابل للتعقب)، والشراكة السرِّيَّة، والشهادات الرقمية، خاتم التوقيت الرقمي، والاتِّصالات الإِلكترونية، والقمار عن بُعد. . . وأي عدد من التنويعات المدهشة التي يجريها الأكاديميون والعلماء والتجّار وزعران الشّيفرة. ونتيجة لهذه الجهود، غدا المفتاح العام موجوداً في كل زمان ومكان، على كل نسخة من برامج نيتسكيب ولوتس نوتس وجزء لا يتجزأ من ويندوز وماكينتوش، وحتماً في محفظة كل شخص، ولا فضل في ذلك للمجتمع المغلق، إنما الفضل كله يعود إِلىٰ المجتمع المفتوح.

هل كان على القيادة العامة للاتِّصالات، وشركائها العمل بجد أكثر لجعل هذه الأفكار قابلة للتطبيق؟ هل كان من الممكن أن يأتوا ببعض من هذه الابتكارات؟ ربما، لكن بينما من السهل إلقاء اللوم على المجتمع الاستخباراتي لعدم تطبيق أفكارهم الأصلية، هناك جانب آخر للقصَّة.

بالنظر إليها من وجهة نظر الأَمن القومي، كان توخي الحذر أمراً منطقياً. ذلك أن تطبيق نظام جديد كلياً في القطاع الخاص، واستخدام أي نوع من التشفير لضمان المعلومات يُعدّ إبداعاً بحد ذاته. لكن القيام بمثل هذا في ما يتصل بأسرار الحكومة، وهي أَنظمة يعتمد عليها توفير الحماية في مواقف خطيرة تتصل بحياة الناس أَو موتهم، إنما يطرح نوعاً آخر من المخاطرة. يقول ويليامسون: «على الحكومة أن تلتزم بأشد الحذر. فالأمان في بعض هذه الأمور، أشد أهمية بكثير من النقل، التحويلات المصرفية، أَو الاتِّصالات عبر الإنترنيت، أَو كيف سيبدو التصميم الجديد لسيارة فورد. لو أنني على قمة

الهرم في ذلك الوقت، هل كنت أجرؤ على تطبيقه؟ ما هو احتمال أن يجد أحدهم البرغي السحري الذي يفكّ كل شيء؟».

كذلك لا يقدِّم ويليامسون أي اعتذار، لقصور مجتمع الاستخبارات عن اكتشاف أي ابتكار عظيم، من تلك الابتكارات التي تمخضت عن المفهوم الأصلي لنظام المفتاح المجزأ. وتذهب الحجة إلىٰ أن القيادة العامة للاتِّصالات كانت بشكل أساسي وكالة للتجسّس والأمن، ولم يكن لديها اهتمام في تطوير ذلك النوع من التقنية التي ستوفر منافع للشعب عموماً (حتَّى ولو كان الشعب هو الذي يدفع رواتبهم). ويقول ويليامسون: «هناك أساس جوهري للأشياء التي على الحكومة القيام بها، أما الأمور الأخرى فربما من الأفضل أن يقوم بها القطاع الخاص». وكان السبب الوحيد لاستمرار الوكالة في العمل على هذه التقنيات هو أن تتبين ما إذا كان بإمكانها، تحسين نوع النشاطات التي تؤديها القيادة العامة للاتِّصالات أصلاً.

لكن بإعراض القيادة العامة للاتِّصالات، عن استغلال التشفير غير السري، كان الاحتمال قائماً بأن رجال الاستخبارات يفوتون الفرصة الهامة للاستفادة منه. وفي عام 1982، وبعد سنوات كثيرة من حصول القيادة العامة للاتِّصالات على جميع المعلومات التي تحتاجها لتطبيق نظام المفتاح العام، واجهت الوكالة البريطانية واحدة من أسوأ الفضائح التي ألمّت بها، عندما باع موظف يدعى جيفري برايم معلومات خطيرة إلىٰ الروس. وفي تلك الفترة الزمنية الطويلة، عانت وكالة الأَمن القومي كذلك من عدة إخفاقات أمنية كبيرة في قضايا شائنة تورطت فيها عائلة والكر، وكريستوفر وأندرولي. واشتملت هذه على نقل مواد هامة لا تُقدَّر بثمن وهذا ما كان ليحصل في نظام يعتمد المفتاح العام. لذلك لم يكن أمراً مفاجئاً حقاً أن تتعرّض الوكالتان لفضيحة على هذا النحو. فبعد كل شيء، فإن الصعوبة في حماية المفاتيح [التقليديَّة] كانت

مشكلة معروفة تماماً. وفي الحقيقة، تلك كانت هي المشكلة التي شرع جيمس إلليز في حلّها.

لذلك لماذا لم تتحرّك الوكالتان على نحو حاسم لاكتشاف بدائل لأنظمتها مبنية على التشفير غير السري؟ في التقديرات النهائية كان التشفير غير السرّي انحرافاً كبيراً عن القاعدة، وينطوي على المجازفة ـ وهما ميزتان عند المتنصت، ومدعاة للفزع عند البيروقراطي. ويقول مالكولم ويليامسون: «عليك أن تتذكّر، أن هذه هيئة حكومية. أعني أن هذا [التشفير غير السرّي]، أمر جديد ومختلف. «فلنضرب عنه صفحاً، لنتجاهله. ولندفعه إلىٰ ما تحت السجادة».

هل شعر العلماء، لدى القيادة العامة للاتّصالات بأنّهم قد خدعوا لدى رؤيتهم الآخرين يحصلون على التقدير على أمر كانوا هم الذين اكتشفوه أصلاً؟ إنهم يدعون بأنّهم لا يشعرون بذلك، ويعتقدون أنّهم يتحدّثون كذلك نيابة عن جيمس إلليز في هذه النقطة. يقول كوكس الذي يشعر بارتياح تام لهذا الوضع: «لقد حصل إلليز على اعتراف داخلي. وذلك أمر تقبله [حين عمل في القيادة العامة للاتّصالات]. الاعتراف داخل الوسط هو كل ما تناله».

كذلك يرفض ويليامسون فكرة أن صمتهم كان النهاية الفجّة، لصفقة فاوستية أبرمت عندما دخلوا عالم الظلال. ويرى العكس، إذ يعتبر أن المتضررين هم الكريبتوجرافيين الذين لا يعملون لصالح الحكومة. ويقول: «إني أتساءل أحياناً لماذا يعمل الناس في الخارج بالكريبتوجرافيا. وما هي أسبابهم؟ من الواضح، أن لدى الحكومات أسباباً وجيهة لذلك، إنها تريد أن تكفل الأمن لاتّصالاتها، وهي تريد الاطلاع على اتّصالات الدول الأخرى. وهذه وظائف هامة. من الذي يريد الجلوس في الجامعة ويقوم بمثل هذه الأمور؟ إنها نوعاً ما مثل كونك بنّاء سفن وتصرّ على العيش في آيوا». [ولاية داخلية بعيدة عن البحر. هـ. م.] (ويليامسون نفسه، بعد سنوات من العمل في القطاع الخاص، هو الآن مواطن أمريكي ـ وقد عاد إلىٰ عالم الظلال، إذ يعمل

لدى مؤسَّسة أبحاث لا تتوخى الربح تقوم بأعمال دفاعية سرِّيَّة).

لكن يبدو أن جيمس إلليز كان قد فكَّر في مستقبل أيامه. ويقول نيك باترسون: «كان عمله الوظيفي لا يؤدي إلىٰ أي هدف، وأحسب أنَّه كان محبطاً وأخذ يتأمّل عمله كما تأمّل خيبة أمله في اختراعه السابق في مجال الراديو». في عام 1985 كتب بحثاً خصيصاً ليطلع الجمهور على حقيقة من اخترع فعلاً كريبتوجرافيا المفتاح العام. وفي الفقرات الافتتاحية، شرح أنَّه مع أن للسرِّيَّة أهمية حاسمة جداً في عمله، إلاَّ أن هناك ظروف يمكن فيها تنحيتها جانباً «في سبيل الدقة التاريخية، بعد أن ظهر جلياً أنه ما من مكاسب أخرى يمكن الحصول عليها من ديمومة السرِّيَّة». ولهذا يتابع قائلاً: «أضحى من المناسب الآن رواية القصة».

من الواضح، أنَّه كان يأمل في تثبيت دعاواه. ينتهي البحث بالتأكيد، لأي شخص بليد الذهن قد تفوته الفكرة، أنه «بعد فترة من القيام بالعمل الأساسي» قام ديفي وهيلمان بما اسماه، إعادة اكتشاف تقنيات التشفير غير السري. لكن إذا كان إلليز قد أمل بأن تجد روايته طريقها إلىٰ خارج المجتمع المغلق بسرعة، فإنه سيتعرَّض لخيبة أمل مريرة. فقد مرّت سنوات وسنوات وظلّت محاولته لوضع الأمور في نصابها طي الكتمان. إذ شعر رؤساؤه أن الوقت لم يحن بعد لإحقاق الحق. ولم يكن الوقت قد حان، بعد خمس سنوات من كتابتها أَو عشر سنوات.

إذن لماذا سمحوا أخيراً للأوراق أن ترى النور في كانون الأول/ ديسمبر 1997، بعد اثنتي عشرة سنة من كتابة إلليز لتاريخ التشفير وقرابة عشرين سنة من العصف الدماغي الذي كان سيهز الكريبتوجرافيا ذاتها؟ يقول كليف كوكس أن الدافع لذلك كان خطبة من المفترض أن يلقيها قرابة ذلك الوقت، تتحدَّث عن موضوعات تشبه ما سيطلق عليه دوماً اسم خوارزمية رسا. لكن مالكولم

ويليامسون، كان أشد صراحة في هذا الموضوع، إذ يقول: أن أوراق البحث كانت جاهزة إلاّ أنه لا يمكن نشرها «حتّى يتقاعد الشخص المعني».

يبدو أن ذلك التقاعد قد حدث، قبل 23 كانون الأول/ ديسمبر 1997، عندما نشرت القيادة العامة للاتّصالات الأوراق الأصلية لكل من إلليز وكوكس وويليامسون على موقع الويب التابع لها، بالإضافة إلىٰ «تاريخ التشفير غير السري» الذي كتبه إلليز عام 1985. لكن النشر أتى متأخراً بالنسبة لإلليز. فلم يكد يمضي شهر على معرفة لعالم بإنجازه العظيم، حتّى كان جيمس هـ. إلليز قد مات.

لكن لم يكن ذلك، قبل أن يلتقي بنظيره في «المجتمع المفتوح». كان هويت ديفي لسنوات كثيرة، يتساءل عن الإشاعات التي تقول بأن كريبتوجرافيا المفتاح العام تم اكتشافها فعلاً على يد الأشباح. وفي أواخر السبعينات، كان لدى مدير وكالة الأَمن القومي بوبي إنمان وجهة نظر عندما أعلم الكريبتوجرافي جس سيمونز، الذي كان يكتب مادة الكريبتوجرافيا لصالح الموسوعة البريطانية، أنه كان من ابتكار وكالة الأَمن القومي. وفي إحدى المرات ألح ديفي على نائب مدير وكالة الأَمن القومي هوارد روزنبلوم للحديث في هذا الموضوع، ودهش حين لم يحله روزنبلوم إلىٰ شخص داخل السياج الثلاثي وإنما إلىٰ مهندس في القيادة العامة للاتّصالات البريطانية لم يسبق له أن سمع به من قبل. ودون أن يفصح عن غرضه ـ إذ كان يأمل أنه سيكون واضحاً ـ اتصل بإلليز، الذي أشار إلىٰ أنه قد يطيب له أيضاً اللقاء معه.

في شهر أيلول/ سبتمبر 1982، كان ديفي قد خطّط لرحلة إلىٰ باريس، وسمح له جدول الرحلة بزيارة إلىٰ تشيلتنهام. كان ديفي وزوجته ماري فيشر قد غادرا باريس على أصوات الترانيم الكنسية، التي كانت تصدح من كل جهاز راديو وتلفزيون، مرافقة لمراسم جنازة الأميرة جريس أميرة موناكو. طار ديفي

وفيشر إِلىٰ مطار هيثرو وذهباً إِلىٰ سالزبوري لقضاء عطلة نهاية الأسبوع. ثم قاد ديفي سيارته وحيداً إِلىٰ تشيلتنهام.

كان إلليز يسكن في أطراف المدينة؛ وخلف منزله كانت الأرض منحدرة، ويمكن للمرء أن يرى منظراً جميلاً للمدينة على مرمى النظر. وقد أطلق على منزله اسم ديلكوشا، التي تعني بالفارسية «المتعة الصغيرة». وكان يربي النحل في حديقة منزله. وفي ذلك الحين، كان إلليز في أواخر الخمسينات من عمره طويل القامة انتشر الشيب في شعره. وكانت زوجته سيدة لطيفة؛ ولديهما ابنة على وشك الالتحاق بكلية الاقتصاد بجامعة لندن. وبعد حديث قصير مع زوجة إلليز، اتجه ديفي وإلليز إِلىٰ إحدى الحانات.

استدار ديفي نحو إلليز بعد أن ركن السيارة. وقال: «أخبرني كيف ابتكرت «التشفير غير السرّي»».

فسأله جيمس إلليز: «من يقول أنني قمت بذلك؟».

فأعطاه ديفي اسم المسؤول في وكالة الأَمن القومي.

فسأله إلليز: «أتعمل عنده؟» فأجاب ديفي بالنفي. إذ لم يكن طرفاً في أي مجتمع مغلق.

وبعد عدد من الأسئلة والأجوبة، أدرك ديفي أن إلليز، لم يكن مستعداً للخوض في هذا الأمر. وبالفعل، تقابل ديفي وإلليز عدة مرات بعد ذلك. وفيما كان من الممكن لهما أن يقتربا جداً من مناقشة الموضوع، لم يكن إلليز ليكشف القصة تماما» مثلما فعل ذلك بوضوح في أبحاثه. لكن العالمين أصبحا بعد ذلك صديقين. وبعد أن تعرّفت زوجة ديفي على إلليز أكثر فأكثر، أصبح بمقدورها أن ترى بوضوح، الصلة بين إلليز وزوجها، وتقول ماري فيشر: «كان كلاهما صوفياً».

من يدري ماذا كان يجول في ذهن جيمس إلليز ذلك اليوم؟ فقد كان

رجلاً وقع على فكرة ثورية وعاش ليرى الآخرين، يفوزون بالشهرة لإعادة اكتشافها؛ وتجشم عناء كتابة بحث يعرض لمساهمته وانتظر، بلا جدوى، لكي ينشر في حياته، إنه ذلك الرجل الذي رأى فكرته، عندما قدمها الآخرون، لم تزدهر فحسب بل خُلقت صناعة جديدة ومجتمعاً جديداً أيضاً، وأحدثت تحولاً جذرياً في الموضوع، نقلة نوعية لدرجة أن عالم الظلال لم يعد هو نفسه. إلاً أنه لم يكن بمقدوره، ولم يكن ليقوم بذلك، أن يخرق القوانين، ويكشف عن أسراره للآخرين، ولا حتّى لقرينه في القطاع الخاص.

وفي تلك الحانة، ظل إلليز يدفع بصاحبه ديفي، لأن يشرب حتّى الثمالة، بينما كانا يتحدثان في كل أمر وموضوع، إلاً الشأن الذي جمع بينهما وأحكم الوثاق بينهما إلىٰ الأبد. ولكن قبل أن ينهي الحديث في الموضوع لم يتمالك إلليز نفسه عن الاعتراف بلباقة، بقول يزيد عن مجلدات، في أمر العالم الذي عاش فيه وعالم الكريبتوجرافيا الذي كان ديفي يعمل على إقامته.

فقال أبو التشفير غير السري لأبي كريبتوجرافيا المفتاح العام: «لقد أفدتم مما عملنا نحن». ثم لزم الصمت محافظاً على سره.

هوامش

نواة هذا الكتاب سلسلة من المقابلات الشخصية أجريتها بين 1992 و2000. وطوال تلك الفترة، قمت بحضور مؤتمرات، وزيارة مواقع رئيسة على الشبكة، وإنجاز نسخة خاصة بي من مخابرات الإشارة، مستخدماً الإمكانات الضخمة التي توفرها الإنترنيت لجمع المعلومات. (وكان رصد المناقشات على موقع sci.crypt أو cypherpunk@toad.com عملاً بكل معنى الكلمة). بالإضافة إلىٰ النصوص المنشورة، فقد اشتملت قائمة المراجع على وثائق من الحكومة والمحاكم ومذكرات، وكذلك مذكرات وتقارير صادرة عن الشركات.

المتفرد

إضافة إلىٰ المقابلات والاتّصالات الشخصية، تم إكمال مادة ديفي بمفكرات غير منشورة تتعلّق بسيرته الذاتية:

«Personal Memories on the Discovery of Public Key Cryptography,» July 1981.

الصفحة

(22) المصادر التي تبحث في أصول الكريبتوجرافيا التقليدية، تتضمّن:

Kahn, The Codebreakers.

وكذلك:

Dorothy Denning, Cryptography and Data Security; Gaines, Cryptanalysis; Wrixton, Codes and Ciphers; Gustavus J. Simmons, «Cryptography» entry in the Encyclopaedia Britannica.

(23) The Codebreakers, P. 146.

(28) عرض لها بشكل واف في:

Hodge, Turing: The Enigma.

ثمة وحدة إنجيما في المتحف القومي الكريبتولوجي في ماريلاند.

(31) إن كتاب:

Bamford, The Puzzle Palace

هو أدق دراسة تبحث في وكالة الأمن القومي. وقد قامت صحيفة The Baltimore Sun بنشر سلسلة من المقالات، محقّقة تحقيقاً علمياً، بقلم توم باومان وسكوت شن بعنوان:

«America's Fortress of Spies,» December 3-15, 1995.

(33) «NSA Employees Security Manual,» reprinted in Phrak, No. 45, March 30, 1994.

(35) «إن المجمع بأكمله، محاط بسياج حلزوني، يبلغ ارتفاعه عشرة أقدام، مكلّل بصفوف متعددة من الأسلاك الشائكة... وفي داخله هناك سياج آخر، مؤلّف من خمسة مناصب رفيعة من أسلاك التوتر العالي، متصلة بأعمدة خشبية، مثبتة حول المبنى، في طبقة من الحصى الإسفلتي الأخضر. أخيراً، هناك سياج حلزوني مرتفع آخر، يدعم السياجين الآخرين».

(38) يمكن مطالعة عمله بأكمله في:

N. J. A. Sloane and Aaron D. Wyner, Shannon: Collected papers, Los Alamitos, CA, IEEE Press, 1993.

(46) Bamford, The Puzzle Palace, p. 168.

اعتمد بامفورد على أبحاث الجنرال مارشال واس. كارتر للتحقق من محاولات وكالة الأمن القومي إلغاء كتاب كاهن.

(49) رسالة هويت ديفي بواسطة البريد الإلكتروني إلى إريك جونفبولث في 25 نيسان/ أبريل 1999.

(52) المعلومات حول فريدمان مستقاة من:

Kahn, The codebreakers; Lambrosd. Callimahos, «The Legendary William F. Friedman,» Cryptologia, vol. 15, No. 3, July 1991, P. 219.

(54) Bruce Schneier, Applied Cryptography, P. 29.

المعيار

على الرغم من جميع ما كُتب حول معيار تشفير البيانات DES، لم يتوفر على الإطلاق عرض موسع، بكل ما في الكلمة من معنى لتطوره. وقد ألقى والت توتشمان كلمة تم تنقيحها بعنوان:

«A Brief History of the Data Encryption Standard,» in Internet Besieged, pp. 275-280.

هناك مقاطع مفيدة حول معيار تشفير البيانات في:

Bamford, The Puzzle Palace; Deffic, Privacy on the Line; Kahn on Codes; Schneier and Banisar, The Electronic Privacy Papers; Schneier, Applied Cryptography.

وقد أعانتني عدة مذكرات داخلية في آي. بي. إم في تصنيف التواريخ، وتوفير معلومات تفصيلية.

الصفحة

(68) Whitfield Diffie, «Preliminary Remarks on the National Bureau of Standards Proposed Standard Algorithm for Computer Data Protection,» May 1975.

(70) المعلومات حول سيرة هذه الشخصية المبدعة متناثرة.

Diffie, Privacy on the Line.

يفي بالغرض.

(71) David Kahn, unpublished notes on an interview. with Feistel, March 29, 1976.

(71) Diffie, Privacy on the Line, P. 57.

(71) Alan Konheim.

(72) Horst Feistel, «Cryptography and Computer Privacy,» Scientific American, vol. 228, No. 5, May 1973, PP. 15-23.

(73) أخبر فايشتل ديفي بأن جون لين الباحث في مختبرات واطسون هو من طلع بهذا الاسم

(85) «A Study of the Lucifer Crypto-Algorithm,» August 18, IBM Memorandum, 1973.

(89) بينما كان المهندسون في كينجستون يستخدمون عادة المقطع الوحيد هذا، فإن الرياضيين في واطسون كانوا لا ينقطعون عن الإشارة إليه بـ «ديز» Dee-Ee-Ess

(94) «The Data Encryption Standard and Its Strength Against Attacks,» IBM Research Journal, Vol. 38, No. 3, May 1994.

(106) U. S. Senate, Select Committee on Intelligence, Unclassified Summary: Involvement of the NSA in the Development of the Data Encryption Standard (1997).

(107) E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, New York, Springer-Verlag, 1993.

(107) M. Matsui, «Linear Cryptanalysis Method for DES Cipher,» Advances in Cryptology: Proceedings of Eurocrypt' 93, New York: Spring-Verlag, 1994.

المفتاح العام

الأبحاث الرئيسية هي:

Diffie and Hellman, «New Directions in Cryptography» (IEEE Transactions on Information Theory, Vol. IF 22, No. 6, November 1976); Merkle, «Secure Communications Under Insecure channels» (Communications of the ACM, Vol. 21, No. 4, 1978).

يورد ديفي بعض المعلومات التاريخية في:

«The First Ten Years of Public Key Cryptography» (in Simmon, Contemporary Cryptography) and «Personal Memories».

بعض الوصوفات التقنية حول كيفية عمل الخوارزميات الحقيقة في:

Bruce Schneier, Applied Cryptography and Garfinkel, PGP.

الصفحة

(124) Diffie, Whitfield and Martin Hellman, «Multiuser Cryptographic Techniques,», Proceedings of the AFIPS National Computer Conterence, 1976, PP. 109-12.

(135) Diffie, «First Ten Years of Public Key Cryptography», op. cit.

البداية

الصفحة

(154) Adi Shamir, «Cryptography: Myths and Realities,» ICAR Distinguished Lecture, delivered at Crypto' 95, August 30, 1995.

(156) Len Adleman, «Algorithmic Number Theory- The Complexity Contribution». Unpublished Paper.

(157) المصدر السابق.

(162) تم تنقيحها وطباعتها لاحقاً بعنوان:

R. A. Rivest, A. Shamir, and L. Adleman, «A Method for Obtaining Digital Signature and Public Key Cryptosystems,» Communications of the ACM, Vol. 21 (2), PP. 120-26, February 1978.

(166) «A New Kind of Cipher That Would Take Millions of Years to Break,» Scientific American, Vol. 237, No. 2, August 1977.

(168) U. S. Senate, Select Committee on Intelligence, Subcommittee on Intelligence and the Rights of Americans, Foreign Intelligence Surveillance Act of 1978, Hearings, Ninety-fifth Cong Second Sess. (1978). Bamford, The Puzzle Palace.

يوفر ملخصاً موجزاً لتحقيقات شامروك وتشيرتش.

(170) كشف عما جرى في المؤسسة القومية للعلوم في:

U. S. Hose of Representatives, Committee of Government Operations, Government Infromation, and Individual Rights Subcommittees, the Governments Classification of Private Ideas, Ninety-Sixth Cong. Second Sess. (1980). Bamford, Diffie and Landau and Gina Bari Kolata, «Computer Encryption and the National Security Agency Connection,» Science, Vol. 97, July 29, 1977, PP. 438-40.

يصف الأنشطة أيضاً.

(174) كانت المقالة:

«Crime Deternent Transponder System,» Transactions on Aerospace and Electronics Systems Vol. 7, No. 1, January 1971.

(175) Deborah Shapley and Gina Kolata, «Cryptology: Scientists Puzzle over Threat to Open Research, Publication,» Science, Vol. 197, September 30, 1977, PP. 1345-349.

(176) Malcolm Browne, «Scientists Accuse Security Agency of Harassment Over Code Studies,» New York Times, October 18, 1977.

(179) A. Shamir, «Cryptography: Myths and Realities,» Op. Cit.

(180) Deborah Shapley, «DOD Vacillates on Wisconsin Cryptography work,» Science, Vol. 20, July 14, 1978, P. 141, Louis Kruh,

«Cryptology and the Law-VII,» Cryptologia, Vol. 10, No. 4, October 1986, P. 248.

وكذلك:

Bomford, The Puzzle Palace, PP. 449-50.

(182) Deborah Shapley, «NSA Slaps Secrecy Order on Inventor's Communications Patent,» Science, Vol., 201, September 8, 1978, PP. 891-94.

كذلك:

Louis Kruh «Cryptology and the Law-VII,» Science, «DOD Vacilates...». Bamford, The Puzzle Palace, PP. 446-51.

(183) بيام قدّم في:

U. S. House of Representatives, committee of Government Operations, Government Information, and Individual Rights Subcommittee, the Government's Classification of Private Ideas, hearing cited abone. Ninety-sixth Cong., Second Sess. (1980).

(185) John M. Harmon, «Constitutionality Under the First Amendment of ITAR Restrictions of Public Cryptography,» memo to Dr. Frank Press, Science advisor to the president, May 11, 1978. Reprinted in Hoffman's Building in Big Brother.

(188) يدعى دان سيلفر

(190) Deborah Shapley, «Intelligence Agency Chief Seeks 'Dialogue with Academics,» Science, Vol. 202, October 27, 1978, pp. 407-9.

(191) تم إعادة طبع الخطاب الذي ألقاه إنمان في جمعية القوات المسلحة للاتّصالات والإلكترونيات بعنوان:

«The NSA Perspective on Telecomunications Protection in the Nongovernmental

Sector» in Schneier and Banisar's the Electronic Privacy Papers, P. 347.

(194) «The Case Against Restraints on Non-governmental Research in Cryptography,» reprinted in Cryptologia, Vol. 5, No. 3, July 1981, P. 143.

الترويج للشيفرة

بعض هذه المادة مستمد من وثائق وصحف مسجلة على شريط مغناطيسي وتعود إلىٰ بدايات خوارزمية رسا RSA، وقد وفرها جيم بيدزوس. كما أن هناك عرضاً جيداً لنشوء خوارزمية رسا في:

Garfinkel, P 6 P.

الصفحة

(201) Diffie, «The First Ten Years of Public Key Cryptography,» Op. cit.

(203) Diffie, Pricacy on the Line, P. 283.

براءات ومفاتيح

(147) Bob Davis, «A Supersecret Agency Finds Selling Secrecy to others Ins't Easy», Wall Street Journal, March 28, 1988.

(248) المسؤول هو ديفيد مكمايز رئيس الأركان لشؤون أمن المعلومات.

(258) A. Shamir, R. A. Rivest and L. Adleman, «Mental Poker,» MIT/LCS Technical Memo 125, February 1979.

(259) A. Shamir, «How to Sahre a Secret,» Communications of the ACM, Vol. 24, No. 11, Novembe 1979, PP. 612-13.

ينسب إلىٰ كل من شامير وجي. آر. بلاكي الفضل في هذا الابتكار.

(259) A. Shamir, Lecture at Securicom'89, quoted in Schneier's Applied Cryptography, P. 92.

(260) «Zero Knowledge and the Department of Defence,» Notices of the American Mathematical Society, (Special Article Series), Vol. 33, No. 1 (1988), PP. 5-12.

(261) John Markoff, «Paper on Codes Is Sent Despite U. S. Objections,» New York Tiemes, August 9, 1989.

(277) «A Proposed Fedral Information Processing Standard for the Digital Signature Standard (DSS),» Federal Register, Vol. 56, August 1991, p. 169.

(279) NIST memo, «Twenty-third Meetings of the NIST/NSA Technical Working Group,» March 18, 1991.

(279) Diffie, Privacy on the Line, P. 74.

(283) قدم ريفيست ملاحظاته في مؤتمر: Computer, Freedom and Privacy Conference لعام 1992.

(284) للاطلاع على أصول توجيهات قرارات الأمن القومي NSDD 145 راجع:
Diffie, Privacy on the Line. Schneier and Banisar, The Electronic Privacy Papers. Tom Athanasion, «Encryption: Technology, Privacy, and National Security,» Technology Review, August-September 1986.

(285) Clinton Brooks, Memo, April 28, 1992.

(286) إن مذكرة التفاهم الموقعة بين مدراء المؤسّسة القومية للمعايير والتكنولوجيا «بشأن تطبيق القانون العام 100 ـ 235» أعيد طبعها في
Schneier and Banisar, The Electronic Privacy Papers, PP. 401-4.

(286) «Communications nications Privacy: Fedral Policy and Actions,» GAO/OSI-92-2-3 (November 1993).

(287) U. S. House of Representatines, Economic and Commercial Law Subcommittee, The Threat of Foreign Economic Espionage to U. S. Corporations, April 29 and May 7, 1992, 102e Congress, Second Sess.

فوضى التشفير

اعتمدت في كتابة بعض أجزاء هذا الفصل على مقالاتيّ السابقتين:
«Crypto Rebels,» Wired, May/ June 1993, and «E-Money (That's What I Want),» Wired, December, 1994

الصفحة

(296) المعلومات بشأن خلفية تشارلي ميريت مستقاة جزئياً من:
Garfinkel, PGP and Maureen Harrington, «Cyber Rebel,» Denver Post, March 3, 1996.

(304) تم التحقق من أن دبليو. إتش. موري في: Jim Warnen, «Is Phil Zimmermann Being Persecuted? Why? By Whom? Who's Next?» Micro Times, April 1995.

(306) المصدر السابق.

(313) Jon Lebkowsky, «The Internet Code Ring,» Fringeware Review, No. 9, January 1995.

(318) Salley Bedell Smith, Diana in Search of Herself, New York, Signet, 2000, P. 247.

(318) Gorden Forbes, «Helmet Radios Give Scrambling New Meanings» USA Today,» April 7, 1994.

(322) حديث جيلمور أعيد طبعه بعنوان:
«Preserving Privacy in America,» Intertek, Vol. 3, No. 2, Summer, 1991.

(325) أعيد طبعه في:

(327) Ludlow, High Noon on the Electronic Frontier, PP. 237-39.

(328) تم إرسال بيان زعران العالم التخيلي إلىٰ قائمة خدمة زعران الشّيفرة في الخامس من تشرين الأول، أكتوبر 1993.

(331) «Crypto and Avoidance of Business Information Anarchy,» Speech to the ACM Conference on Computer and Communication Security, November, 1993.

(333) David Chaum, editor, Smart Carel 2000, North Holland, 1991.

(340) David Chaum, «The Dining Cryptographer's Problem: Unconditional Sender and Receiver Untraceability,» Journal of Cryptology, Vol. 1, NO. 1, 1988, PP. 56-75.

(343) رسالة مات ثوميلينسون إلىٰ قائمة خدمة زعران الشّيفرة في 30 كانون الثاني/ يناير 1994.

(344) ثمة بحث جيد في:

Jonathan D. Wallace, «Nameless in Cyberspace: Anonymity on the Internet,» Cato Breifing papers, No. 54, December 8, 1999.

(344) أعيد طبع رسالة ماي في:

Ludlow, High Noon on the Electronic Frontier, PP. 241-44.

(345) «Crypto and Avoidance,» op. cit.

رقاقة المقراض:

معظم المعلومات الواردة في هذا الفصل مستقاة من مقابلات شخصية وأعداد وفيرة من الوثائق التي أتيحت للجمهور، وقد أمدّني بها EPIC أو جون جيلمور. وكان العرض المعاصر لمعركة المقراض الذي اعتمدته هو:

«The Cypherpunks vs. Uncle Sam,» Sunday New York Times Magazines, June 12, 1994.

ثمة مقالة مفيدة أخرى هي:

Bob Davis, «Clipper Chip Is Your Friend,» Wall Street Journal, March 22, 1994.

الصفحة

(355) تم تلخيص اجتماعات مجموعة العمل التقني في مذكرة (أضحت أجزاء منها متاحة للجمهور الآن). وفي أول لقاء تم عقده في فورت ميد في الخامس من أيار/ مايو 1989، أطلقت المؤسّسة القومية للمعايير والتكنولوجيا على المفتاح العام اسم «القضية الأولى لمجموعة العمل التقني».

(356) إن أعمال القمة والمقراض عرض لها مفصلاً في:

Dorothy Denning, «The Clipper Encryption System,» American Scientist, Vol. 81, July-August 1993.

(359) Lyn McNulty, NIST Memo, «Summary of 7/23-24/92 Off-Site Meeting,» July 27, 1992.

(363) David Stipp, «Techno-Hero or Public Enemy,» Fourtune, November 11, 1996.

(366) «Jackboots on the Infobahn» reprinted in Ludlow's High Noon on the Electronics Frontier, pp. 207-13.

(367) J. R. Davis, «Use of Clipper Chip in At & T TSD 3600 During Phase of Production», memo to Sessions, December 23, 1992.

(368) وثيقة للاطلاع مرسلة إلى تينيت في 19 شباط/ فبراير 1993.

(373) «Telecommunications Overview» prepared by the FBI's Advanced Telephony Unit.

(380) «Jackboots on the Infobahn», reprinted in Ludlow's High Noon on the Electronic Frontier, pp. 207-13.

(330) انظر:

Steven Levy, «Clipper Chick», Wired, September 1996.

(380) Sterling, The Hacker Crackdown, p. 299.

(381) «Statement by the Press Secretary», The White Houses April 16, 1993.

(382) John Markoff, «New Communication System Stirs Talk of Privacy vs. Eavesdropping», April 16, 1993.

(384) Steven Levy, «Uncle Sam».

(385) «Sink the Clipper», New York Times, February 4, 1994.

(386) عدل خطاب بيكر بعنوان:

«Don't Worry be Happy: Why Clipper Is Good For You», in Wired, June 1994.

(386) E.F. Brickell, D. E. Denning, S.T. Kent, D.P. Maher, and W. Tuchman, «Skipjack Review - Interim Report», unpublished, July 28, 1993.

(387) Silvio Micali, «Fair Cryptosystems», Technical Memo, Laboratory for Computer Science, MIT, august 21, 1992.

(388) Levy, «Uncle Sam...».

(389) Tim May, «The Coming Police State».

رسالة موجهة إلى قائمة خدمة زعران الشيفرة في 9 آذار/ مارس 1994.

(389) U.S. Senate, Committee on the Judiciary, Subcommittee on Technology and the law, Clipper Chip Key Escrow Encryption Program, hearings, May 3, 1994, 103d congress, Second Sess.

(396) John Markoff, «Flaw Discovered in Fedral Plan For Wiretapping», New York Times, June 2, 1994.

بحث بليز حول عيوب المقراض:

«Protocol Failure in the Escrowed Encryption Standard», Proceedings of the Second ACM Conference on Computer and Communications Security, November, 1994.

(398) Philip Elmer-Dewitt, «Who Should Keep the Keys?» Time, march 14, 1994.

(401) U.S. House of Representatives, Committee on Foreign Affairs, Subcommittee on Economic Policy, Trade and Environment, Export Controls on Mass Market Software, Hearings, October 12, 1993, 103d Congress, First Sess.

(407) أعيد طبعه في:

Schneier and Banisar, The Electronic Privacy Papers, p. 692.

جر الخطى نحو التشفير

إن بعض المعلومات الواردة في هذا الفصل مستقاة من مقالتي:

«Wisecrakers», Wired, April 1996.

الصفحة

(414) Robert Morris, «Ways of Losing Information», Invited Lecture at Crypto' 95, August 29, 1995.

(420) Giles Brassard, crypto Bytes, vol. 1, No. 1, Spring, 1995.

(437) David Bank, «The Keys to the Kingdom», San Jose Mercury News, June 27, 1994.

(440) القيود المفروضة على تصدير سوق البرمجيات.

(444) روايات حول مذكرة التفتيش يعرض لها:

Wendy M. Crossman, «Alt.scientology,war,» Wired, December 1995. Wallace and Morga, Sex, Laws, and Cyberspace.

(448) وردت الرواية بأكملها في:

«How Digicash Blew Everything,»

المنشورة أصلاً في الصحيفة الهولندية نيكست ماجازين Next! Magazine.

(451) في:

Damand Lin, Cryptography's Rle in Securing the Information Socieyt.

(452) Judge Charles R. Richey, Memorandum Opinion, Karn V. State, CA-95-1812 (D.C.C.), March 22, 1996.

(452) بالإضافة إلى المقابلات الشخصية ووثائق المحاكم، تم استقصاء أصول بيرنشتاين من:

Peter Cassidy, «Reluctant Hero,» Wired, June 1996.

(454) يتضمن سجل المحكمة أشرطة سجلها بيرنشتاين لهذه المحادثات وسواها.

(460) ثمة وصف مفصل للمشروع في:

The Electronic Frontier Foundation's Cracking DES.

(461) قدّم فريد ملاحظاته في مؤتمر: «The Conference on Global Cryptography» المنعقد في 26 أيلول/ سبتمبر 1994.

(465) Mike Godwin, «The New Cryptographic Landscape,» E-Commerce Law Weekly, Vol. 1, No. 1, October 19, 1999.

(467) Don Clark, «Bidzos Holds Key to Guarding Internet Secrets,» Wall Street Journal, April 16, 1996.

(468) لئن كان معظم القضية سرياً، فإن بعض الوثائق متاحة للجمهور في:

RSA Data Security, Inc. vs. Cylink Corporation and Caro-Kann Corporation are public.

(473) الواقع أن اثنتين من براءات اختراع ستانفورد اللتين تغطيان ديفي ـ هيلمان لتبادل المفتاح والحقيبة. (ومفهوم المفتاح العام ذاته على نحو قابل للجدل). كان قد انتهى مفعولهما في عام 1997. وانتهى مفعول براءة اختراع معهد ماساتشوسيتس للتكنولوجيا الذي يغطي خوارزمية رسا RSA في 20 أيلول/ سبتمبر 2000.

خاتمة: السر المكشوف

بعض المعلومات الواردة هنا ظهرت أول مرة في:

Wired, April 1999, «The Open Secret,»

التي كانت أول عرض لمنجزات مجموعة أمن الاتّصالات الإلكترونية LESG. (وكان أن جاء عرض سايمون سينج في: The Code Book لاحقاً). إن بحث إيلي:

«The Story of Non-Secret Encryption»

يضع الخطوط العامة للاكتشافات، وشأنه شأن أبحاث مجموعة أمن الاتّصالات الإلكترونية LESG الأخرى، متوفر في موقعها على الإنترنيت. بعض ملاحظات كليفورد كوكس الواردة هنا مستقاة من:

«The Invention of Non-Secret Encryption,»

وهي كلمة تم إلقاؤها في بليتشلي بارك في 20 حزيران/ يونيو 1998 في ندوة: History of Cryptography التي استضافتها الجمعية البريطانية لتاريخ الرياضيات.

الصفحة

(479) ما زال هذا البحث غير متوفر. وليس من الواضح ما إذا كان هذا البحث متصلاً ببرنامج التشفير الحديث المعروف باسم «المشروع إكس» Project X في مختبرات بيل وفي:

Turing: The Enigma,

يصف آندرو هودجيس مشاركة آلان تورنيتج في ذلك المشروع، التي أفادت أيضاً من المادة التي أدخلها كل من كلود شانون (في مختبرات بيل آنذاك أيضاً) ووليام فريدمان. وإذا ما كان هناك أي تأثير متبادل بين هذه المشاريع، فإن ذلك يعني أن تراث المفتاح العام ينبع مباشرة من الشخصيات البارزة في البلاد في المرحلة ما قبل ظهور المفتاح العام في الشيفرة.

(489) M. J. Williamson, «Non-Secret Encryption Using a Finite Field,» GESG Report, January 21, 1974.

كان مشروع كوكس هو:

«A Not on Non-Secret Encryption,» CESG Report, November, 20, 1973.

(492) M. J. Williamson, «Thoughts on Cheaper Non-Secret Encryption,» CESG Report, August 10, 1976.

(495) قصة برايم في لاحقة كتاب:

Bamford, The Puzzle Palace.

(495) حكاية والكر مقدمة على نحو لطيف في:

Howard Blum, I Pledge Allegiance... New York, Simon & Schuster, 1987.

(495) بويس ولي هما الشخصيتان الرئيستان في:

The Falcon and the Snowman, New York, Simon & Schuster, 1979.

المراجع

Bamford, James, *The Puzzle Palace*. New York: Penguin, 1983.

Bover, Carl B. revised by Uta C. Merzbach. *A History of Mathematics*. Wiley, 1989.

Burham, David. *The Rise of the Computer State*. New York: Random House, 1983.

Campbell, Jeremy. *Grammatical Man: Information, Entropy, Language and Life*. New York: Simon & Schuster, 1982.

Card, Orson Scott. *Ender's Game*. New York: Tor Books, 1985.

Computer Professionals for Social Responsibility. *Cryptography and Privacy Sourcebook*, Years 1991-1993.

Dam, Kenneth, and Herbert Lin, eds., National Research Council. *Cryptography's Role in Securing the Information Society*. National Academy Press, 1996.

Denning Dorothy E. *Cryptography and Data Security*. Reading, MA: Addison-Wesley, 1982.

-, *Information Warfare and Security*. Reading, MA: Addison-Wesley, 1999.

-, and Peter J. Denning. *Internet Besieged*, ACM Press, 1998.

Diffie, Whitfield, and Susan Landua. *Privacy on the Line*. Boston: MIT Press, 1998.

Electronic Frontier Foundation. *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design*. Sebastopol, CA: O'Reilly, 1998.

Electronic Privacy Information Center. *Cryptography and Privacy Sourcebook*. Years 1994-1998.

Gaines, Helen Fouche. *Cryptanalysis*. New York: Dover, 1939.

Gardner, Martin. *Penrose Tiles to Trapdoor Ciphers*. New York: Freeman, 1989.

Garfinkel, Simpson. *PGP: Pretty Good Privacy*. Sebastopol, CA: O'Reilly, 1995.

Godwin, Mike. *Cyber Rights*. New York: Times Books, 1998.

Hodges, Andrew. *Turing: The Enigma*. New York: Simon & Schuster, 1983.

Hoffman, Lance, ed. *Building Big Brother*. New York: Springer-Verlag, 1995.

Kahn, David. *The Codebreakers: The Story of Secret Writing*. New York: Macmillan, 1967.

-, *Kahn on Codes: Secrets of the New Cryptology*. New York: Macmillan, 1983.

Kelly, Kevin. *Out of Control*. Reading, MA: Addison Wesley, 1994.

Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

Levy, Stephen. *Hackers: Heroes of the Computer Revolution*. New York: Double-day, 1984.

Ludlow, Peter, ed. *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*. Boston: MIT Press, 1996.

Rosenheim, Shawn James. *The Cryptographic Imagination: Secret Writing from Edgar Poe to the Internet*. Baltimore, MD: Johns Hopkins University Press, 1997.

Schneier, Bruce. *Applied Cryptography*, second edition. New York: Wiley, 1996.

and David Banisar, eds. *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance*. New York: Wiley Computer Publishing, 1997.

Simmons, Gustavus J., ed. *Contemporary Cryptography: The Science of Information Integrity*. New York: IEEE Press, 1992.

Singh, Simon. *The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*. New York: Doubleday, 1999.

Sterling, Bruce. *The Hacker Crackdown*. New York: Bantam, 1993.

Wallace, Jonathan D., and Mark Mangan. *Sex, Laws, and Cyberspace*. New York: Holt, 1996.

Wrixon, Fred B. *Codes and Ciphers*. Englewood Cliffs, NJ: Prentice-Hall, 1992.

Zim, Herbert T. *Codes and Secret Writing*. New York: Morrow, 1948.

المصطلحات

- **القمة (Capstone)** رقاقة مصمّمة من وكالة الأَمن القومي ذات قدرات تشفيرية عالية، كما أنّها توفر توقيعاً رقمياً، بذات القدرة، إنما مع مفتاح مودع بحيث تستطيع السلطات قراءة الرسائل المشفّرة.
- **شيفرة (Cipher)** تعرف بخوارزمية تشفير أيضاً، وهي الدالة (التابع) الرياضي المستخدم في تشفير الرسائل، وفكّ تشفيرها.
- **نصّ مشفَّر (Ciphertext)** وضع رسالة (يفترض بأنّها غير قابلة للقراءة) بعد تشفيرها.
- **رقاقة المقراض (Clipper Chip)** نظام وديعة المفتاح، من تصميم وكالة الأَمن القومي، وهو مخصّص لأَجهزة الهاتف. ولا تقدم هذه الرقاقة المنيعة إِلاَّ التشفير ونظام وديعة المفتاح جزء في نظام القمة (Capstone).
- **أمن الاتّصالات (Communications Security-COMSEC)** إجراء التثبت من قوة وسلامة رموز الشّيفرة. (وهذا نصف المهمة المناطة بوكالة الأَمن القومي، بالإِضافة إِلىٰ الإِشارة SIGINET.
- **تحليل الشّيفرة(Cryptoanalysis)**: تفكيك الشّيفرة ـ فن السحر الأسود الذي يعمل على تحويل نص معمى، إِلىٰ نص واضح دون استخدام المفتاح.
- **الكريبتوجرافيا الكتابة بالشّيفرة (Cryptography)**: استخدام الرموز السرّيّة والشّيفرة.
- **الكريبتوجرافيا علم الشّيفرة (Cryptology)**: دراسة ورياضيات الرموز السرّيّة والشّيفرة. وتستخدم أحياناً مرادفاً للكريبتوجرافيا.
- **نظام التشفير (Crypto System)**: وسيلة لتشفير البيانات والتوابع الكريبتوجرافية الأخرى.

- **معيار تشفير البيانات (Data Encryption Standard «DES»)**: نظام تشفير مطوَّر من IBM عن نظام لوسيفر Lucifer الأسبق. ومع أنّه كان عرضة لنقد النقاد أصلاً، إلاّ أنه ثبتت متانته، فلا ينال منه شيء، سوى ما اعتبره النقاد ضعفاً في امتداد، أو طول المفتاح.
- **مبادلة ديفي ـ هيلمان لتبادل المفتاح (Diffie-Hellman Key Exchange)**.
- **مبادلة مفتاح ديفي ـ هيلمان**: خوارزمية ابتكرها هويت ديفي ومارتي هيلمان ويسمح لشخصين بتوليد مفتاح سري، على نحو يسمح لكل منهما بامتلاكه، دون أن يتمكن من تنصت على المكالمة، بأن يركب مفتاحاً خاصاً به.
- **التوقيع الرقمي (Digital Signature)**: بيانات مشفَّرة رياضية المصدر لتثبيت هوية المرسل.
- **خوارزمية التوقيع الرقمي، (Digital Signature Algorithm)**: (DSA) خوارزمية نشرتها وكالة الأَمن القومي، وقد نصحت باعتمادها معياراً. وهذه الخوارزمية تختلف عن توقيع الـ رسا بعدم قدرتها على تشفير المعلومات.
- **تشفير (Encryption)**: تعمية المعلومات (بتحويلها إِلىٰ نصوص مشفَّرة) لمنع قراءتها عند اعتراضها.
- **التحليل إِلىٰ عوامل (Factoring)**: عملية رياضية تقوم على اكتشاف العدد الحاصل عن ضرب عددين أصغر منه واكتشاف الأعداد الأصلية الدالة (التابع) وحيدة الاتجاه هي أساس خوارزمية الرسا.
- **دالة (تابع) التجميع (Hash Function)**: طريقة كريبتوجرافية لتكثيف رسالة توفر خلاصة النص الأصلي.
- **إيديا (IDEA)**: خوارزمية تشفير البيانات الدولية استخدمت في النسخ المتأخرة من برنامج «بي جي بي»، منتهى السرية وحلّت محل باس أو ماتيك الأصلية.
- **مفتاح (Key)**: مكون نظام تشفير يحدِّد طريقة تعمية الرسالة. وحين يطبق المفتاح على النص الواضح يتحول إِلىٰ نص مشفَّر؛ كما أن المفتاح ذاته (أَو في نظام المفتاح العام، نصف المفتاح المماثل من زوج المفاتيح)، يعيد الرسالة إِلىٰ نصها الصريح الأصلي.
- **وديعة المفتاح (Key Escrow)**: طريقة مختصر، أَو باب سري موضوع قصداً في أَنظمة الشّيفرة ليمكن السلطات من تفكيك الرسائل بسرعة، للحيلولة دون تعريض الأمن للخطر، كما يزعم.
- **طول المفتاح (Key Length)**: تزداد صعوبة تفكيك الشّيفرة بطريقة القوة الغاشمة (اختبار كل احتمال حتّى ظهور النص الواضح) بمدى طول المفتاح. ويعرف مجال المفاتيح المحتملة بمدى المفتاح. والجهد الذي يتطلبه الهجوم بالقوة الغاشمة هو عامل التشغيل.

- **الحقيبة (Knapsack)**: من أوائل نظام المفتاح العام للتشفير ابتكره رالف ميركل، ثم أمكن تفكيكه لاحقاً.
- **لوسيفر (Lucifer)**: نظام تشفير تقليدي ابتكره هورست فايشتل في مختبرات الآي بي إم، في أوائل السبعينات. وكان الأساس لمعيار تشفير البيانات (1975).
- **الحل لمرة واحدة (One Time Pad)**: الشكل الوحيد من الشّيفرة، الذي يصمد أمام محاولة التفكيك رياضياً، إذ يتطلب مفتاحاً، بمثل مدى الرسالة ذاتها، ولا يمكن تكراره.
- **الدالة/ التابع وحيدة الاتجاه (One Way Function)**: عملية رياضية سهلة الحساب، ولكن عكسها صعب جداً. للباب السري وحيد الاتجاه ميزة أخرى هي أن من يملك المعلومات الصحيحة قادر على عكس الحساب.
- **النص الواضح (Plaintext)**: النص الأصلي الصريح قبل التشفير.
- **منتهى السرِّيَّة (Pretty Good Privacy «PGP»)**: نظام شيفرة شائع ابتكره فيل زيمرمان، وقام بتوزيعه مجاناً على الإنترنيت عام 1991.
- **المفتاح الخاص (Private Key)**: المفتاح الخاص في نظام المفتاح العام، وهو أحد زوجين من المفاتيح، ولا بد من الحرص عليه؛ إنه المفتاح الوحيد الذي يمكن به تفكيك الرسائل التي شفِّرت بالمفتاح العام كما يمكن لصاحبه أن يوقّع به الرسائل لإثبات أن صاحب التوقيع هو مرسلها حقاً.
- **المفتاح العام (Public Key)**: أحد المفتاحين اللذين يسمحان بإرسال رسائل خاصة، سرِّيَّة إلىٰ صاحبه. كذلك يستخدم المفتاح، للتحقّق من التوقيع الرقمي. ويمكن توزيع هذا المفتاح على نطاق واسع دونما المجازفة بالأمن.
- **كريبتوجرافيا المفتاح العام (Public Key Cryptography)**: نظام ابتكره ديفي وهيلمان في عام 1975.
- **مولِّد أرقام عشوائية (Random Number Generator «RNG»)**: جزء من نظام شيفرة يعتمد على الكومبيوتر ويجعل الطريقة التي تعمى بها المفاتيح، الرسالة عصية على التوقع.
- **آر سي 2، آر سي 4 (RC 2, RC 4)**: شيفرات تقليدية ابتكرها رون رايفست (آر س RC: شيفرات رايفست).
- **مدور البريد/ الرسائل (Remailer)**: خدمة تقدمها شبكة الإنترنيت تسمح بتوجيه رسائل إلكترونية دون الكشف عن اسم المرسل.
- **خوارزمية رسا (RSA Algorithm)**: أكثر أنظمة الشيفرات القائمة على المفتاح العام شيوعاً، ابتكرها رايفست وشامير وأدليمان.

- **مخابرات الإشارة SIGINT (Signal Intelligence)**: وسائل اعتراض أشكال التخابر وتفكيك الشّيفرة عند الضرورة.
- **سكيبجاك (الوثاب) (Skip Jack)**: شيفرة قوية تقليدية من ابتكار وكالة الأَمن القومي، وهي في صميم شيفرات القمة والمقراض.
- **المفتاح المتماثل (Symmetrical Key)**: مفتاح يستخدم في الكريبتوجرافيا التقليديَّة، يستخدم المرسل أحدهما لتعمية النص ويستخدم المستقبل الآخر لفك الرسالة.

الفهرس

كانت الكريبتوجرافيا ـ استخدام الرموز السرية ـ حتى عهد قريب المملكة المقدسة لعباقرة الأحاجي وجواسيس الحكومة. ولكن قبيل شيوع الانترنيت ظهرت زمرة خارج السرب من الغرباء عن هذه المنطقة فأطلقوا ثورة في هذا الحقل الذي كان ذات يوم منطقة محرمة. وكان ما أبدعوه من أدوات جبارة في الرياضيات، على حد تعبير لورنس ليسيج أستاذ القانون بجامعة هارڤارد «أهم انطلاقة تكنولوجية في السنوات الألف الأخيرة». وقدر لهذه الخوارزميات الهائلة التي ابتكروها أن تأتي بالحل للمشكلة العويصة التي تواجهنا جميعاً في القرن الحادي والعشرين، كيف يخاطب أحدنا الآخر، ونجري أعمالنا التجارية، ونحفظ معلوماتنا الخاصة بنا في عالم متشابك تتقاطع خطوطه. لكن هذه كانت ثورة أراد الجواسيس ورجال مكتب التحقيقات الفيدرالي إخمادها في المهد...

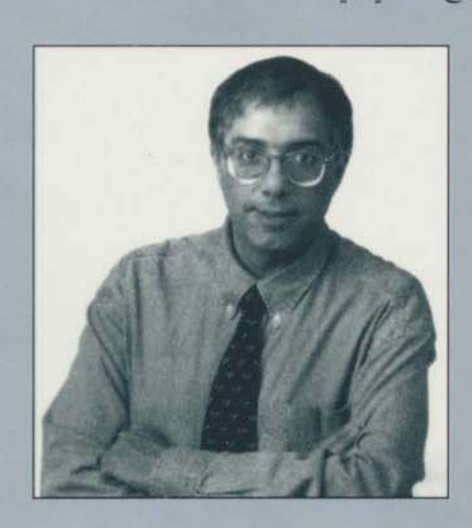
في هذه الرواية الكاملة التي تقدم لأول مرة عن حرب الشيفرة العظمى التي هزت عصر الكومبيوتر، يقدم محرر القضايا التكنولوجية في مجلة نيوز ويك وصاحب الكتب الأكثر رواجاً ستيڤن ليڤي بإسهاب، الخطوط الرئيسة لثورة كريبتوجرافيا «الشعب» وصدامها مع حكومة الولايات المتحدة. ويدور كتاب الشيفرة حول موضوع السرية في عصر المعلوماتية، والجريئين وأصحاب الرؤى الذين تنبؤوا قبل عشرين عاماً بأن أفضل ما في الانترنيت ـ حرية الوصول إلى المعلومات ـ هو أخطر مثلب فيها أيضاً: احتمال نهاية السرية.

يروي هذا الكتاب قصة «ثوار الشيفرة» الشجعان بأسلوب مؤثر كقصة واقعية مشوقة، ومزيج ممتع من حكايا العباقرة في عملهم، والخيال العلمي، والتآمر السياسي، كما يقدمها صوت مرشد متمكن عارف بالتكنولوجيا والسياسة والثقافة الرقمية. وهناك وايت ديڤي، ذو الشعر الطويل الذي يعتبر «نيوتون» الشيفرة، والذي أبتكر حل «المفتاح العام» المذهل،

وديڤيد تشوم الذي هدد بأسلوب «الأموال الرقمية المغفلة» الأسس المالية للعالم كله؛ و« زعران الشيفرة» أمثال فيل زيمرمان الذي نشر الشيفرة التي تعادل بمتانتها ما تتمتع به الشيفرة العسكرية للولايات المتحدة من مِنْعَةٍ وسرّبها تحت أنف الحكومة الأمريكية. ويطالع القارئ، بعد، أول رواية عن نوايا وكالة الأمن القومية الخفية من صنع «رقاقة المقراض» وكيف خربت إدارة كلينتون العملية.

بالإضافة إلى ذلك، فإن ليڤي يتقصى ما بات يعتبر تطوراً حاسماً في حروب الشيفرة، التحالف الغريب بين عباقرة الإليكترونيات والشركات العملاقة. والهدف الذي يجمع بينهم : الدفاع عن حقوقنا في حماية أسرارنا الخاصة من تدخل الحكومة والمتطفلين.

إن كتاب **«الشيفرة»** كتاب رائد يعرض فيه مؤلفه الذي جعل من قراصنة الكمبيوتر كلمة شائعة في كل بيت، أحدث قضية في المجال الإليكتروني. إنه مرجع أساسي في مجاله.



ستيڤن ليڤي، مؤلف «قراصنة الكمبيوتر»، و«هائل إلى حد الجنون»، و«الحياة الاصطناعية» و«سر وحيد القرن»، والكاتب الرئيسي في قسم التكنولوجيا بمجلة نيوز ويك، ويساهم في مجلة وايرد منذ صدورها. ويعيش مع زوجته وابنه في نيويورك.

بعض ما قيل في كتاب «الشيفرة»

«لم تكن الشيفرة المدنية، قد وجدت بعد تقريباً قبل ثلاثة عقود من الزمن. أما الآن فليس بوسعنا أن نسحب الأموال من رصيدنا من كوى الصراف الآلي أو أن نقوم بعملية شراء عبر شبكة الانترنيت دونها. وإنها لخدمة جليلة أن تُروى قصتها، ومنّة أن تكون الرواية ممتعة لكل من له صلة بالشيفرة، أي في هذه الأيام يعني كلنا جميعاً. إن «الشيفرة» كتاب كنا بحاجة لأن يُكتب، وقد قام ستيفن ليڤي بالمهمة».

نيل ستيفنسون، مؤلف كتاب Cryptonomicon

«لا بد لك من سماع قصة العباقرة المتمردين والأبطال الذين هبوا من حيث لا ندري، وكيف قاموا بتحرير الشيفرة رغماً عن أنوف الأشباح وعمدوا إلى وضع الشيفرة عند محققي الأحلام من شارات الدوت ـ كوم. إن الكتابة بالشيفرة لم تجعل التجارة الإليكترونية أمراً ممكناً وحسب، بل إنها أول حركة سياسية في العصر الرقمي. فطالع المستقبل في هذا الكتاب.

كيفن كيللي، مؤلف New Rules for The New Economy و Out of Control

---

أخيراً! القصة الإنسانية المؤثرة للكشوفات التي منحتنا التجارة الإليكترونية والسرية على الانترنيت. لقد كتب ستيفن ليڤي الكريبتوجرافيا روح آلة جديدة.

ديڤيد كاهن، مؤلف The Code Breakers

ردمك : ISBN 9960-40-127-8

موضوع الكتاب: أمن الكومبيوتر/كريبتوجرافيا

موقعنا على الانترنت:
http://www.obeikanbooks.com